日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００３年　８月　７日
出願番号 Application Number: [ST. 10/C]:	特願２００３－２８９４３３ [ＪＰ２００３－２８９４３３]
出願人 Applicant(s):	松下電器産業株式会社

２００３年　９月　４日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０７２５２７

【書類名】　特許願
【整理番号】　2030750074
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 15/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　高山　久
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　古山　純子
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100109553
　【弁理士】
　【氏名又は名称】　工藤　一郎
【先の出願に基づく優先権主張】
　【出願番号】　特願2002-245997
　【出願日】　平成14年 8月26日
【先の出願に基づく優先権主張】
　【出願番号】　特願2003- 72284
　【出願日】　平成15年 3月17日
【手数料の表示】
　【予納台帳番号】　100322
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0214408

【書類名】特許請求の範囲
【請求項１】
ユーザは電子バリューを保有し、前記電子バリューにはユーザが指定した電子バリューに対する認証情報(VPW)に不可逆演算処理(F)を施したバリュー認証情報(F(VPW))が暗号化された状態で含まれており、ユーザが前記電子バリューの正しい保有者であることを認証する処理において、認証側が乱数(R)を生成してユーザ側に送信し、ユーザ側はユーザが入力した電子バリューに対する認証情報(VPW')からバリュー認証情報(F(VPW'))を生成し、更に、前記乱数(R)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R,F(VPW')))を生成して、前記電子バリューと前記認証情報(G(R,F(VPW')))を認証側に送信し、認証側が受信した電子バリューの暗号を復号化して、電子バリューからバリュー認証情報(F(VPW))を取り出し、前記乱数(R)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R,F(VPW)))を生成し、前記受信した認証情報(G(R,F(VPW')))と前記生成した認証情報(G(R,F(VPW)))が一致することを検証してユーザを認証することを特徴とする認証方式。
【請求項２】
前記電子バリューの暗号化されている部分の復号化鍵は、バリュー認証情報(F(VPW))を不可逆演算処理(H)したデータ(H(F(VPW)))とマスター鍵とから生成した鍵であり、ユーザが前記電子バリューの正しい保有者であることを認証する処理において、ユーザ側が更にバリュー認証情報(F(VPW'))に不可逆演算処理(H)を行いデータ(H(F(VPW')))を生成して、前記電子バリューと前記認証情報(G(R,F(VPW')))と共に認証側に送信し、認証側が受信したデータ(H(F(VPW')))とマスター鍵とから復号化鍵を生成して、受信した電子バリューの暗号を復号化することを特徴とする請求項１記載の認証方式。
【請求項３】
ユーザは電子バリューを保有し、前記電子バリューにはユーザが指定した電子バリューに対する認証情報(VPW)に不可逆演算処理(F)を施したバリュー認証情報(F(VPW))が暗号化された状態で含まれており、認証側はユーザが前記電子バリューの正しい保有者であり、ユーザも認証側を認証する相互認証処理において、認証側が乱数(R1)を生成してユーザ側に送信し、ユーザ側はユーザが入力した電子バリューに対する認証情報(VPW')からバリュー認証情報(F(VPW'))を生成し、更に、乱数(R2)を生成して、更に、前記バリュー認証情報(F(VPW'))と前記乱数(R1)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R1,F(VPW')))を生成して、前記電子バリューと共に認証情報(G(R1,F(VPW')))と乱数(R2)を認証側に送信し、認証側が受信した電子バリューの暗号を復号化して、電子バリューからバリュー認証情報(F(VPW))を取り出し、前記乱数(R1)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R,F(VPW)))を生成し、前記受信した認証情報(G(R,F(VPW')))と認証情報(G(R,F(VPW)))とが一致することを検証してユーザを認証し、更に、バリュー認証情報(F(VPW))と乱数(R1)と乱数(R2)とを組み合わせたデータに不可逆演算処理(I)を行い認証情報(I(R1,R2,F(VPW)))を生成してユーザ側に送信し、ユーザ側がバリュー認証情報(F(VPW'))と乱数(R1)と乱数(R2)とを組み合わせたデータに不可逆演算処理(I)を行い認証情報(I(R1,R2,F(VPW')))を生成し、前記受信した認証情報(I(R1,R2,F(VPW)))と認証情報(I(R1,R2,F(VPW')))とが一致することを検証して認証側を認証することを特徴とする相互認証方式。
【請求項４】
前記電子バリューの暗号化されている部分の復号化鍵は、バリュー認証情報(F(VPW))を不可逆演算処理(H)したデータ(H(F(VPW)))とマスター鍵とから生成した鍵であり、認証側はユーザが前記電子バリューの正しい保有者であり、ユーザも認証側を認証する相互認証処理において、ユーザ側が更にバリュー認証情報(F(VPW'))に不可逆演算処理(H)を行いデータ(H(F(VPW')))を生成して、前記電子バリューと認証情報(G(R1,F(VPW')))と乱数(R2)と共に認証側に送信し、認証側が受信したデータ(H(F(VPW')))とマスター鍵とから復号化鍵を生成して、受信した電子バリューの暗号を復号化することを特徴とする請求項３記載の相互認証方式。

【請求項５】
ユーザは電子バリューを保有し、前記電子バリューにはユーザが指定した電子バリューに対する認証情報(VPW)に不可逆演算処理(F)を施したバリュー認証情報(F(VPW))が暗号化された状態で含まれており、認証側が前記電子バリューの有効性を検証し、電子バリューの内容を更新する更新処理において、認証側が乱数(R1)を生成してユーザ側に送信し、ユーザ側はユーザが入力した電子バリューに対する認証情報(VPW')からバリュー認証情報(F(VPW'))を生成し、更に、乱数(R2)を生成して、更に、前記バリュー認証情報(F(VPW'))と前記乱数(R1)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R1,F(VPW')))を生成して、前記電子バリューと共に認証情報(G(R1,F(VPW')))と乱数(R2)を認証側に送信し、認証側が受信した電子バリューの暗号を復号化して、電子バリューからバリュー認証情報(F(VPW))を取り出し、前記乱数(R1)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R1,F(VPW)))を生成し、前記受信した認証情報(G(R1,F(VPW')))と認証情報(G(R1,F(VPW)))とが一致することを検証してユーザを認証し、更に、内容を更新した電子バリューを生成し、更に、バリュー認証情報(F(VPW))と乱数(R1)と乱数(R2)とを組み合わせたデータに不可逆演算処理(I)を行い認証情報(I(R1,R2,F(VPW)))を生成して、前記内容を更新した電子バリューと認証情報(I(R1,R2,F(VPW)))とをユーザ側に送信し、ユーザ側がバリュー認証情報(F(VPW'))と乱数(R1)と乱数(R2)とを組み合わせたデータに不可逆演算処理(I)を行い認証情報(I(R1,R2,F(VPW')))を生成し、前記受信した認証情報(I(R1,R2,F(VPW)))と認証情報(I(R1,R2,F(VPW')))とが一致することを検証して認証側を認証し、電子バリューを前記受信した内容を更新した電子バリューに更新することを特徴とする更新処理方式。
【請求項６】
前記電子バリューの暗号化されている部分の復号化鍵は、バリュー認証情報(F(VPW))を不可逆演算処理(H)したデータ(H(F(VPW)))とマスター鍵とから生成した鍵であり、認証側が前記電子バリューの有効性を検証し、電子バリューの内容を更新する更新処理において、ユーザ側が更にバリュー認証情報(F(VPW'))に不可逆演算処理(H)を行いデータ(H(F(VPW')))を生成して、前記電子バリューと認証情報(G(R1,F(VPW')))と乱数(R2)と共に認証側に送信し、認証側が受信したデータ(H(F(VPW')))とマスター鍵とから復号化鍵を生成して、受信した電子バリューの暗号を復号化することを特徴とする請求項５記載の更新処理方式。
【請求項７】
電子バリューを格納する記憶手段を備え、ユーザが入力した前記電子バリューに対する認証情報(VPW')に不可逆演算処理(F)を施してバリュー認証情報(F(VPW'))を生成し、更に、前記バリュー認証情報(F(VPW'))と認証装置から受信した乱数(R)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R,F(VPW')))を生成して、前記電子バリューと認証情報(G(R,F(VPW')))を認証装置に送信することで、ユーザが前記電子バリューの正しい保有者であることの認証を受けることを特徴とする携帯端末。
【請求項８】
電子バリューを格納する記憶手段を備え、ユーザが入力した前記電子バリューに対する認証情報(VPW')に不可逆演算処理(F)を施してバリュー認証情報(F(VPW'))を生成し、更に、乱数(R2)を生成し、更に、前記バリュー認証情報(F(VPW'))と認証装置から受信した乱数(R1)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R1,F(VPW')))を生成して、前記電子バリューと認証情報(G(R1,F(VPW')))と乱数(R2)を認証装置に送信することで、ユーザが前記電子バリューの正しい保有者であることの認証を受け、また、バリュー認証情報(F(VPW'))と乱数(R1)と乱数(R2)とを組み合わせたデータに不可逆演算処理(I)を行い認証情報(I(R1,R2,F(VPW')))を生成し、前記認証装置から受信した認証情報(I(R1,R2,F(VPW)))と認証情報(I(R1,R2,F(VPW')))とが一致することを検証して前記認証装置を認証することを特徴とする携帯端末。
【請求項９】
電子バリューを格納する記憶手段を備え、ユーザが入力した前記電子バリューに対する認

証情報(VPW')に不可逆演算処理(F)を施してバリュー認証情報(F(VPW'))を生成し、更に、乱数(R2)を生成し、更に、前記バリュー認証情報(F(VPW'))と認証装置から受信した乱数(R1)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R1,F(VPW')))を生成して、前記電子バリューと認証情報(G(R1,F(VPW')))と乱数(R2)を認証装置に送信することで、ユーザが前記電子バリューの正しい保有者であることの認証を受け、また、バリュー認証情報(F(VPW'))と乱数(R1)と乱数(R2)とを組み合わせたデータに不可逆演算処理(I)を行い認証情報(I(R1,R2,F(VPW')))を生成し、前記認証装置から受信した認証情報(I(R1,R2,F(VPW)))と認証情報(I(R1,R2,F(VPW')))とが一致することを検証して前記認証装置を認証し、前記電子バリューを前記認証装置から受信した電子バリューに更新することを特徴とする携帯端末。

【請求項１０】

前記電子バリューの暗号化されている部分の復号化鍵は、バリュー認証情報(F(VPW))を不可逆演算処理(H)したデータ(H(F(VPW)))とマスター鍵とから生成した鍵であり、前記携帯端末がバリュー認証情報(F(VPW'))に不可逆演算処理(H)を行いデータ(H(F(VPW')))を生成して、前記電子バリューと前記認証情報(G(R,F(VPW')))とデータ(H(F(VPW')))を認証装置に送信することで、ユーザが前記電子バリューの正しい保有者であることの認証を受けることを特徴とする請求項７から請求項９のいずれか一に記載の携帯端末。

【請求項１１】

前記記憶手段には電子バリューごとに設定された属性情報であるプロパティが前記電子バリューと共に格納され、前記電子バリューによる認証処理の際に前記プロパティに基づいて設定された任意の動作を行うことを特徴とする請求項７から請求項１０のいずれか一に記載の携帯端末。

【請求項１２】

前記記憶手段には電子バリューごとに設定された属性情報であるプロパティが前記電子バリューと共に格納され、前記電子バリューによる認証処理の際に前記認証装置から受信したユーザ端末制御情報と前記プロパティに基づいて任意の動作を行うことを特徴とする請求項７から請求項１０のいずれか一に記載の携帯端末。

【請求項１３】

乱数(R)を生成して携帯端末に送信し、前記携帯端末から認証情報(G(R,F(VPW')))と電子バリューとを受信し、電子バリューの暗号化されている部分の暗号を復号化して、前記電子バリューの有効性を検証し、更に、前記電子バリューからバリュー認証情報(F(VPW))を取り出し、前記乱数(R)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R,F(VPW)))を生成し、受信した認証情報(G(R,F(VPW')))と生成した認証情報(G(R,F(VPW)))とが一致することを検証して、ユーザを認証することを特徴とする認証装置。

【請求項１４】

乱数(R1)を生成して携帯端末に送信し、前記携帯端末から認証情報(G(R1,F(VPW')))と電子バリューと乱数(R2)とを受信し、電子バリューの暗号化されている部分の暗号を復号化して、前記電子バリューの有効性を検証し、更に、電子バリューからバリュー認証情報(F(VPW))を取り出し、前記乱数(R1)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R1,F(VPW)))を生成し、受信した認証情報(G(R1,F(VPW')))と生成した認証情報(G(R1,F(VPW)))とが一致することを検証してユーザを認証し、更に、バリュー認証情報(F(VPW))と乱数(R1)と携帯端末から受信した乱数(R2)とを組み合わせたデータに不可逆演算処理(I)を行い認証情報(I(R1,R2,F(VPW)))を生成し、ユーザ側に前記認証情報(I(R1,R2,F(VPW)))を送信して携帯端末による認証を受けることを特徴とする認証装置。

【請求項１５】

乱数(R1)を生成して携帯端末に送信し、前記携帯端末から認証情報(G(R1,F(VPW')))と電子バリューと乱数(R2)とを受信し、電子バリューの暗号化されている部分の暗号を復号化して、前記電子バリューの有効性を検証し、更に、電子バリューからバリュー認証情報(F(VPW))を取り出し、前記乱数(R1)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R1,F(VPW)))を生成し、受信した認証情報(G(R1,F(VPW')))と認証情報(G(R1,F(VPW

)))とが一致することを検証してユーザを認証し、更に、内容を更新した電子バリューを生成し、更に、バリュー認証情報(F(VPW))と乱数(R1)と携帯端末から受信した乱数(R2)とを組み合わせたデータに不可逆演算処理(I)を行い認証情報(I(R1,R2,F(VPW)))を生成し、ユーザ側に前記更新した電子バリューと認証情報(I(R1,R2,F(VPW)))を送信して、携帯端末上の電子バリューを前記更新した電子バリューに更新することを特徴とする認証装置。

【請求項１６】

前記電子バリューの暗号化されている部分の復号化鍵は、バリュー認証情報(F(VPW))を不可逆演算処理(H)したデータ(H(F(VPW)))とマスター鍵とから生成した鍵であり、前記認証装置が前記携帯端末から受信したデータ(H(F(VPW')))とマスター鍵とから復号化鍵を生成して、受信した電子バリューの暗号を復号化することを特徴とする請求項１３から請求項１５のいずれか一に記載の認証装置。

【請求項１７】

耐タンパなセキュリティモジュールを備え、前記セキュリティモジュールが前記電子バリューの暗号化されている部分の復号化処理を行い、前記セキュリティモジュールに電子バリューのネガリストを格納し、前記受信した電子バリューの有効性を検証する際に前記ネガリストに前記受信した電子バリューがないことを前記セキュリティモジュールが検証することを特徴とする請求項１３から請求項１６のいずれか一に記載の認証装置。

【請求項１８】

前記セキュリティモジュールがセンターと通信して前記セキュリティモジュール内に格納している情報を更新することを特徴とする請求項１７に記載の認証装置。

【請求項１９】

前記電子バリューによる認証処理の際にユーザ端末制御情報を携帯端末に送信して前記携帯端末の動作を制御し、前記携帯端末から受信したサービス端末制御情報に基づいて自らの動作を行うことを特徴とする請求項１３から請求項１８のいずれか一に記載の認証装置。

【請求項２０】

携帯端末から受信した電子バリュー発行要求メッセージからユーザが指定した電子バリューに対する認証情報(VPW)を取り出し、前記電子バリューに対する認証情報(VPW)に不可逆演算処理(F)を施してバリュー認証情報(F(VPW))を生成し、更に前記バリュー認証情報(F(VPW))に不可逆演算処理(H)を施したデータ(H(F(VPW)))とマスター鍵とから暗号鍵を生成し、前記バリュー認証情報(F(VPW))と前記生成した暗号鍵とを用いて電子バリューを生成して、携帯端末に送信することを特徴とする電子バリュー発行サーバ。

【請求項２１】

携帯端末から受信した電子バリュー発行要求メッセージからユーザが指定した電子バリューに対する認証情報(VPW)に不可逆演算処理(F)を施したバリュー認証情報(F(VPW))を取り出し、前記バリュー認証情報(F(VPW))に不可逆演算処理(H)を施したデータ(H(F(VPW)))とマスター鍵とから暗号鍵を生成し、前記バリュー認証情報(F(VPW))と前記生成した暗号鍵とを用いて電子バリューを生成して、携帯端末に送信することを特徴とする電子バリュー発行サーバ。

【請求項２２】

前記電子バリューには、電子バリュー公開情報とセキュリティ情報とが含まれ、前記セキュリティ情報は電子バリュー秘密情報と前記バリュー認証情報(F(VPW))と署名情報とを前記生成した暗号鍵によって暗号化したデータであり、前記署名情報は前記電子バリュー公開情報と前記電子バリュー秘密情報と前記バリュー認証情報(F(VPW))とを連結したデータに対する電子署名であることを特徴とする請求項２０または請求項２１に記載の電子バリュー発行サーバ。

【請求項２３】

前記電子バリューには、電子バリュー公開情報とセキュリティ情報とが含まれ、前記セキュリティ情報は電子バリュー秘密情報と前記バリュー認証情報(F(VPW))と署名情報とを前記生成した暗号鍵によって暗号化したデータであり、前記署名情報は前記電子バリュー公

開情報と前記電子バリュー秘密情報と前記バリュー認証情報(F(VPW)) とを連結したデータに対するハッシュ演算の結果であることを特徴とする請求項２０または請求項２１に記載の電子バリュー発行サーバ。

【請求項２４】

ユーザの信用情報と前記ユーザが指定した電子バリューに対する認証情報(VPW)のリスク評価の結果に基づいてリスク管理情報を生成し、前記電子バリュー秘密情報の中に前記リスク管理情報を組み込むことを特徴とする請求項２２または請求項２３に記載の電子バリュー発行サーバ。

【請求項２５】

ユーザが管理する携帯端末と認証装置と電子バリュー発行サーバとによって構成され、前記携帯端末に前記電子バリュー発行サーバから受信した電子バリューを格納し、前記電子バリューには、ユーザが指定した電子バリューに対する認証情報(VPW)に不可逆演算処理(F)を施したバリュー認証情報(F(VPW))が暗号化された状態で含まれており、ユーザが前記電子バリューの正しい保有者であることを認証する処理において、認証装置が乱数(R)を生成して携帯端末に送信し、携帯端末はユーザが入力した電子バリューに対する認証情報(VPW')からバリュー認証情報(F(VPW'))を生成し、更に、前記乱数(R)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R,F(VPW')))を生成して、前記電子バリューと前記認証情報(G(R,F(VPW')))を前記認証装置に送信し、認証装置が受信した電子バリューの暗号を復号化して、電子バリューからバリュー認証情報(F(VPW))を取り出し、前記乱数(R)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R,F(VPW)))を生成し、前記受信した認証情報(G(R,F(VPW')))と前記生成した認証情報(G(R,F(VPW)))が一致することを検証してユーザを認証することを特徴とする認証システム。

【請求項２６】

前記電子バリューの暗号化されている部分の復号化鍵は、バリュー認証情報(F(VPW))を不可逆演算処理(H)したデータ(H(F(VPW)))とマスター鍵とから生成した鍵であり、ユーザが前記電子バリューの正しい保有者であることを認証する処理において、携帯端末が更にバリュー認証情報(F(VPW'))に不可逆演算処理(H)を行いデータ(H(F(VPW')))を生成して、前記電子バリューと前記認証情報(G(R,F(VPW')))と共に認証装置に送信し、認証装置が受信したデータ(H(F(VPW')))とマスター鍵とから復号化鍵を生成して、受信した電子バリューの暗号を復号化することを特徴とする請求項２５記載の認証システム。

【請求項２７】

ユーザが管理する携帯端末と認証装置と電子バリュー発行サーバとによって構成され、前記携帯端末に前記電子バリュー発行サーバから受信した電子バリューを格納し、前記電子バリューには、ユーザが指定した電子バリューに対する認証情報(VPW)に不可逆演算処理(F)を施したバリュー認証情報(F(VPW))が暗号化された状態で含まれており、認証装置はユーザが前記電子バリューの正しい保有者であり、ユーザも認証装置を認証する相互認証処理において、認証装置が乱数(R1)を生成して携帯端末に送信し、携帯端末はユーザが入力した電子バリューに対する認証情報(VPW')からバリュー認証情報(F(VPW'))を生成し、更に、乱数(R2)を生成して、更に、前記バリュー認証情報(F(VPW'))と前記乱数(R1)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R1,F(VPW')))を生成して、前記電子バリューと共に認証情報(G(R1,F(VPW')))と乱数(R2)を認証装置に送信し、認証装置が受信した電子バリューの暗号を復号化して、電子バリューからバリュー認証情報(F(VPW))を取り出し、前記乱数(R1)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R,F(VPW)))を生成し、前記受信した認証情報(G(R,F(VPW')))と認証情報(G(R,F(VPW)))とが一致することを検証してユーザを認証し、更に、バリュー認証情報(F(VPW))と乱数(R1)と乱数(R2)とを組み合わせたデータに不可逆演算処理(I)を行い認証情報(I(R1,R2,F(VPW)))を生成して携帯端末に送信し、携帯端末がバリュー認証情報(F(VPW'))と乱数(R1)と乱数(R2)とを組み合わせたデータに不可逆演算処理(I)を行い認証情報(I(R1,R2,F(VPW')))を生成し、前記受信した認証情報(I(R1,R2,F(VPW)))と認証情報(I(R1,R2,F(VPW')))とが一致することを検証して認証装置を認証することを特徴とする相互認証システム。

【請求項２８】
前記電子バリューの暗号化されている部分の復号化鍵は、バリュー認証情報(F(VPW))を不可逆演算処理(H)したデータ(H(F(VPW)))とマスター鍵とから生成した鍵であり、認証装置はユーザが前記電子バリューの正しい保有者であり、ユーザも認証装置を認証する相互認証処理において、携帯端末が更にバリュー認証情報(F(VPW'))に不可逆演算処理(H)を行いデータ(H(F(VPW')))を生成して、前記電子バリューと認証情報(G(R1,F(VPW')))と乱数(R2)と共に認証装置に送信し、認証装置が受信したデータ(H(F(VPW')))とマスター鍵とから復号化鍵を生成して、受信した電子バリューの暗号を復号化することを特徴とする請求項２７記載の相互認証システム。
【請求項２９】
ユーザが管理する携帯端末と認証装置と電子バリュー発行サーバとによって構成され、前記携帯端末に前記電子バリュー発行サーバから受信した電子バリューを格納し、前記電子バリューには、ユーザが指定した電子バリューに対する認証情報(VPW)に不可逆演算処理(F)を施したバリュー認証情報(F(VPW))が暗号化された状態で含まれており、認証装置が前記電子バリューの有効性を検証し、電子バリューの内容を更新する更新処理において、認証装置が乱数(R1)を生成して携帯端末に送信し、携帯端末はユーザが入力した電子バリューに対する認証情報(VPW')からバリュー認証情報(F(VPW'))を生成し、更に、乱数(R2)を生成して、更に、前記バリュー認証情報(F(VPW'))と前記乱数(R1)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R1,F(VPW')))を生成して、前記電子バリューと共に認証情報(G(R1,F(VPW')))と乱数(R2)を認証装置に送信し、認証装置が受信した電子バリューの暗号を復号化して、電子バリューからバリュー認証情報(F(VPW))を取り出し、前記乱数(R1)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R1,F(VPW)))を生成し、前記受信した認証情報(G(R1,F(VPW')))と認証情報(G(R1,F(VPW)))とが一致することを検証してユーザを認証し、更に、内容を更新した電子バリューを生成し、更に、バリュー認証情報(F(VPW))と乱数(R1)と乱数(R2)とを組み合わせたデータに不可逆演算処理(I)を行い認証情報(I(R1,R2,F(VPW)))を生成して、前記内容を更新した電子バリューと認証情報(I(R1,R2,F(VPW)))とを携帯端末に送信し、携帯端末がバリュー認証情報(F(VPW'))と乱数(R1)と乱数(R2)を組み合わせたデータに不可逆演算処理(I)を行い認証情報(I(R1,R2,F(VPW')))を生成し、前記受信した認証情報(I(R1,R2,F(VPW)))と認証情報(I(R1,R2,F(VPW')))とが一致することを検証して認証装置を認証し、電子バリューを前記受信した電子バリューに更新することを特徴とする電子バリュー更新システム。
【請求項３０】
前記電子バリューの暗号化されている部分の復号化鍵は、バリュー認証情報(F(VPW))を不可逆演算処理(H)したデータ(H(F(VPW)))とマスター鍵とから生成した鍵であり、認証装置が前記電子バリューの有効性を検証し、電子バリューの内容を更新する更新処理において、携帯端末が更にバリュー認証情報(F(VPW'))に不可逆演算処理(H)を行いデータ(H(F(VPW')))を生成して、前記電子バリューと認証情報(G(R1,F(VPW')))と乱数(R2)と共に認証装置に送信し、認証装置が受信したデータ(H(F(VPW')))とマスター鍵とから復号化鍵を生成して、受信した電子バリューの暗号を復号化することを特徴とする請求項２９記載の電子バリュー更新システム。
【請求項３１】
電子鍵の発行において、携帯端末から受信した電子鍵発行要求メッセージからユーザが指定した電子鍵に対する認証情報(VPW)に不可逆演算処理(F)を施したバリュー認証情報(F(VPW))を取り出し、前記バリュー認証情報(F(VPW))に不可逆演算処理(H)を施したデータ(H(F(VPW)))とマスター鍵とから暗号鍵を生成し、前記バリュー認証情報(F(VPW))と前記生成した暗号鍵とを用いて電子鍵を生成して携帯端末に送信する電子鍵の発行機能と、
電子鍵の認証において、乱数(R)を生成して携帯端末に送信し、前記携帯端末から認証情報(G(R,F(VPW')))と電子鍵とを受信し、電子鍵の暗号化されている部分の暗号を復号化して、前記電子鍵の有効性を検証し、更に、前記電子鍵からバリュー認証情報(F(VPW))を取り出し、前記乱数(R)と組み合わせたデータに不可逆演算処理(G)を行い認証情報(G(R,F

(VPW)))を生成し、受信した認証情報(G(R,F(VPW')))と生成した認証情報(G(R,F(VPW)))とが一致することを検証して、ユーザを認証する電子鍵の認証機能とを
有することを特徴とする錠前装置。
【請求項３２】
電子鍵の発行において、乱数(R0)を生成して携帯端末に送信し、携帯端末から受信した電子鍵発行要求メッセージから、ユーザが携帯端末に入力した錠前番号(LN')と前記乱数(R0)とを組み合わせたデータに不可逆演算処理(J)を施したユーザ識別情報(J(LN',R0))を取り出し、錠前番号(LN)と前記乱数(R0)とを組み合わせたデータに不可逆演算処理(J)を施してユーザ識別情報(J(LN,R0))を生成し、受信したユーザ識別情報(J(LN',R0))と生成したユーザ識別情報(J(LN,R0))とが一致することを検証してユーザを認証し、電子鍵を発行することを特徴とする請求項３１記載の錠前装置。
【請求項３３】
前記発行した電子鍵の鍵ＩＤを格納する記憶手段を備え、電子鍵の認証において、受信した電子鍵の鍵ＩＤと前記記憶手段に格納された鍵ＩＤとの照合処理を行い、
その後、前記携帯端末から受信した認証情報(G(R,F(VPW')))と電子鍵とに基づく認証処理を行う
ことを特徴とする請求項３１又は請求項３２に記載の錠前装置。
【請求項３４】
認証装置に対して認証を求める認証要求装置であって、
前記認証装置が保持する復号鍵により復号化可能な暗号化形式で第一情報を暗号化した暗号化第一情報を取得する暗号化第一情報取得部と、
前記第一情報との関係が所定の関係であるか判断することを目的とする第二情報を取得する第二情報取得部と、
前記暗号化第一情報取得部で取得した暗号化第一情報と、前記第二情報取得部で取得した第二情報とを関連付けて前記認証装置に対して送信する送信部と、
を有する認証要求装置。
【請求項３５】
暗号化第一情報を保持する暗号化第一情報保持部を有し、
暗号化第一情報取得部は、暗号化第一情報保持部にて保持されている暗号化第一情報を取得する請求項３４に記載の認証要求装置。
【請求項３６】
認証を目的とした情報である認証情報を入力するための認証情報入力部と、
前記認証情報入力部から入力された認証情報を加工する認証情報加工部と、
を有し、
前記第二情報は、前記認証情報加工部にて加工された情報である請求項３４又は請求項３５に記載の認証要求装置。
【請求項３７】
前記認証情報加工部は、前記認証情報をハッシュ関数にて加工する請求項３６に記載の認証要求装置。
【請求項３８】
認証要求装置の送信部から送信された暗号化第一情報と、その暗号化第一情報に関連づけて送信された第二情報とを受信する受信部と、
暗号化第一情報の復号化をするための復号鍵を保持する復号鍵保持部と、
受信部で受信した暗号化第一情報を復号鍵保持部に保持されている復号鍵を利用して復号化し第一情報を得る復号化部と、
復号化部で復号化した第一情報と、復号化前の第一情報である暗号化第一情報と関連付けて受信された第二情報と、が所定の関係にあるか判断する判断部と、
を有する認証装置。
【請求項３９】
認証情報を取得する認証情報取得部と、

認証情報取得部で取得した認証情報を利用して前記認証情報と、所定の関係を有するように第一情報を生成する第一情報生成部と、
暗号化の鍵を保持する暗号鍵保持部と、
前記第一情報生成部で生成された第一情報を前記暗号鍵保持部で保持された暗号化の鍵で暗号化する暗号化部と、
を有する情報関連付装置。

【書類名】明細書
【発明の名称】電子バリューの認証方式と認証システムと装置
【技術分野】
【０００１】
本発明は、クレジットカードやデビットカード、会員証、ＩＤカード、チケットなどを電子情報化した電子バリューをユーザの携帯端末に格納し、ユーザが、それらの正しい所有者であることを認証することで、それぞれに対応する物やサービスがユーザに提供されるサービスにおいて、携帯端末が耐タンパ機能のない端末であっても、安全なユーザ認証処理を可能にするものである。
【背景技術】
【０００２】
従来の技術では、安全な認証処理を行う方法として、公開鍵暗号方式に基づく電子署名を用いる方法や、予め登録しておいたＩＤ及びパスワードを照合することで本人を認証する方法があった。例えば、電子署名を用いる方法を携帯電話に適用した場合、耐タンパ機能を備えたＩＣカードモジュールを携帯電話に搭載し、そのＩＣカードモジュールには、予め、公開鍵暗号方式のプライベート鍵と公開鍵の鍵ペアを格納し、例えば、クレジットカードの場合には、その公開鍵を用いたクレジットカードの証明書を携帯電話に格納して、クレジットカードの利用時には、ＩＣカードモジュールがプライベート鍵を用いて電子署名処理を行い、認証側ではその電子署名をクレジットカードの証明書を用いて検証することで、ユーザ認証を行う。一方、ＩＤとパスワードを用いる方法の場合には、携帯電話に耐タンパ機能を備えたＩＣカードモジュールを搭載する必要はないが、予め登録されたＩＤとパスワードとの照合を行うために、認証側にＩＤとパスワードのデータベースが必要となる。（例えば、特許文献１参照）。
【特許文献１】特開２００１－２６５７３５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかし、従来の技術の電子署名を用いる方法の場合には、携帯電話または携帯端末に耐タンパ機能を備えたＩＣカードモジュールを搭載する必要があり、端末コストがアップしてしまうという課題があった。また、ＩＤとパスワードを用いる方法の場合には、認証側にＩＤとパスワードのデータベースが必要となり、例えば、クレジットカード決済などの本人認証に適用するためには、各加盟店に設置されているクレジット決済端末に、クレジットカードの会員のＩＤとパスワードのデータベースを置くか、ネット上にＩＤとパスワードのデータベースを持つセンターを作り、本人認証をする度にセンターにアクセスするといった方法をとる必要がある。前者の場合には、各加盟店のクレジット決済端末に、ＩＤとパスワードのデータベースを置くことは、セキュリティ上問題があり、物理的にも現実的でない。また、後者の場合も、本人認証のためのセンターと各クレジット決済端末間のネットワークを新たに構築する必要がり、また、毎回、本人認証の度にセンターにアクセスする必要があるので、迅速な処理が期待できないという課題があった。
【０００４】
本発明は、こうした従来の問題点を解決するものであり、耐タンパ機能のない携帯端末であっても、安全で高速な認証処理ができ、クレジットカード決済や会員の本人認証、チケットの改札などに適用できる認証方式、及び、その認証方式を応用した各種のシステムを提供し、また、そのシステムを実現する装置を提供することを目的としている。
【課題を解決するための手段】
【０００５】
そこで、上記の目的を達成するため、本発明の認証方式では、ユーザは暗号化された電子バリュー(Encrypt(ev))を保有し、電子バリュー(ev)には、ユーザが指定した電子バリューに対する認証情報(VPW)を第１の不可逆演算処理(F)したバリュー認証情報(F(VPW))が含まれており、ユーザが前記電子バリューの正しい保有者であることを認証する処理にお

いて、認証側が乱数Rを生成してユーザ側に送信し、ユーザ側はユーザが入力した電子バリューに対する認証情報(VPW')からバリュー認証情報(F(VPW'))を生成し、更に、乱数Rと組み合わせたデータに第２の不可逆演算処理(G)を行い認証情報(G(R,F(VPW')))を生成して、暗号化された電子バリューと共に認証側に送信し、認証側が受信した暗号化された電子バリューの暗号を復号化して、電子バリューからバリュー認証情報(F(VPW))を取り出し、乱数Rと組み合わせたデータに第２の不可逆演算処理(G)を行い認証情報(G(R,F(VPW)))を生成し、受信した認証情報(G(R,F(VPW')))と認証情報(G(R,F(VPW)))とが一致することを検証して、ユーザを認証する。本認証方式によれば、ユーザ側に暗号鍵等の秘密情報を格納する必要がなく、耐タンパ機能も必要しないが、認証側では安全にユーザを認証することができる。

【０００６】

また、本発明の認証方式では、暗号化された電子バリューの暗号の復号化鍵は、バリュー認証情報(F(VPW))を第３の不可逆演算処理(H)したデータ(H(F(VPW)))とマスター鍵とから生成した鍵であり、ユーザが前記電子バリューの正しい保有者であることを認証する処理において、ユーザ側が更にバリュー認証情報(F(VPW'))を第３の不可逆演算処理(H)したデータ(H(F(VPW')))を生成して、認証情報(G(R,F(VPW')))と暗号化された電子バリューと共に認証側に送信し、認証側が受信したデータ(H(F(VPW')))とマスター鍵とから復号化鍵を生成して、受信した暗号化された電子バリューの暗号を復号化する。本認証方式によれば、電子バリュー毎に電子バリューを暗号化している暗号鍵が異なるため、仮に、一つの電子バリューの暗号が解かれたとしても、他の電子バリューには影響を与えないので、安全性を高めることが出来る。

【０００７】

また、本発明の認証方式では、電子バリューには、電子バリューの発行者による電子署名が施されており、ユーザが前記電子バリューの正しい保有者であることを認証する処理において、認証側が暗号を復号化した電子バリューに施された電子署名を検証する。本認証方式によれば、電子バリューの偽造を防止することができ、さらに、認証処理の安全性を高めることができる。

【０００８】

また、本発明の認証システムでは、ユーザの携帯端末に暗号化された電子バリュー(Encrypt(ev))を格納し、前記電子バリュー(ev)には、ユーザが指定した電子バリューに対する認証情報(VPW)を第１の不可逆演算処理(F)したバリュー認証情報(F(VPW))が含まれており、ユーザが前記電子バリューの正しい保有者であることを認証する処理において、認証装置が乱数Rを生成して携帯端末に送信し、携帯端末が、ユーザが入力した電子バリューに対する認証情報(VPW')からバリュー認証情報(F(VPW'))を生成し、更に、乱数Rと組み合わせたデータに第２の不可逆演算処理(G)を行い認証情報(G(R,F(VPW')))を生成して、暗号化された電子バリューと共に前記認証装置に送信し、認証装置が受信した暗号化された電子バリューの暗号を復号化して、電子バリューからバリュー認証情報(F(VPW))を取り出し、乱数Rと組み合わせたデータに第２の不可逆演算処理(G)を行い認証情報(G(R,F(VPW)))を生成し、受信した認証情報(G(R,F(VPW')))と認証情報(G(R,F(VPW)))とが一致することを検証して、ユーザを認証する。本認証システムによれば、携帯端末に暗号鍵等の秘密情報を格納する必要がなく、耐タンパ機能を搭載する必要がないが、認証装置では安全にユーザを認証することができる。

【０００９】

また、本発明の認証システムでは、前記暗号化された電子バリューの暗号の復号化鍵は、バリュー認証情報(F(VPW))を第３の不可逆演算処理(H)したデータ(H(F(VPW)))とマスター鍵とから生成した鍵であり、ユーザが前記電子バリューの正しい保有者であることを認証する処理において、携帯端末が更にバリュー認証情報(F(VPW'))を第３の不可逆演算処理(H)したデータ(H(F(VPW')))を生成して、認証情報(G(R,F(VPW')))と暗号化された電子バリューと共に認証装置に送信し、認証装置が受信したデータ(H(F(VPW')))とマスター鍵とから復号化鍵を生成して、受信した暗号化された電子バリューの暗号を復号化する。本

認証システムによれば、電子バリュー毎に電子バリューを暗号化している暗号鍵が異なるため、仮に、一つの電子バリューの暗号が解かれたとしても、他の電子バリューには影響を与えないので、安全性を高めることが出来る。

【００１０】

また、本発明の認証システムでは、電子バリューには、電子バリューの発行者による電子署名が施されており、ユーザが前記電子バリューの正しい保有者であることを認証する処理において、認証装置が暗号を復号化した電子バリューに施された電子署名を検証する。本認証システムによれば、電子バリューの偽造を防止することができ、さらに、認証処理の安全性を高めることができる。

【００１１】

また、本発明の認証システムでは、携帯端末に格納された暗号化された電子バリューは、携帯端末からの電子バリュー発行要求に基づいて電子バリュー発行サーバが生成し、携帯端末にダウンロードされたものであり、電子バリュー発行要求には、ユーザが指定した電子バリューに対する認証情報(VPW)を第１の不可逆演算処理(F)したバリュー認証情報(F(VPW))が含まれ、前記電子バリュー発行サーバがバリュー認証情報(F(VPW))を用いて暗号化された電子バリューを生成する。本認証システムによれば、携帯端末に対して、各種の電子バリューを発行するサービスを行うことが出来る。

【発明の効果】

【００１２】

本発明の電子バリューの認証方式と認証システム及びそれを構成する装置を用いることによって、耐タンパ機能のない携帯端末を利用して、安全な認証処理を行うことができる。

【００１３】

また、電子バリューとして電子クレジットを携帯電話にダウンロードして、携帯電話を用いて安全なクレジット決済を行うことができ、ユーザはクレジットカードを持ち歩く必要がなくなり、利便性が向上する。

【００１４】

また、ユーザは、複数種類の電子クレジットを携帯電話にダウンロードして、その中から電子クレジットを選択して使用することができ、また、クレジット決済端末は、複数種類のクレジットカード及び複数のアクワイアラに対応することができ、しかも、携帯型であるため、例えば、小売店や飲食店などの加盟店の店員がクレジット決済端末を持ち歩くことができ、お客さん（ユーザ）を待たせることなく、売り場やフロアーなどの接客の現場で決済を行うことができる。

【００１５】

また、電子バリューとして電子チケットを携帯電話にダウンロードして、携帯電話を用いて電子チケットの改札処理を行うことができ、ユーザはチケットを入手するために特定の場所に行ったり、郵送してもらったりする必要がなくなり、利便性が向上する。

【００１６】

また、電子バリューとして電子鍵を携帯電話にダウンロードして、携帯電話を用いて錠前装置を開錠または施錠することができ、また、物理的な鍵の受け渡しが発生しないため、ユーザは鍵を管理している所に鍵を取りに行く必要がなく、また、管理する側も鍵の受け渡しを行う担当者を置く必要がなく、業務の効率化を図ることができる。

【００１７】

また、ユーザの管理のもと、錠前装置の電子鍵を複数の携帯電話に対して発行することができ、また、その無効化を行うことができる。従来の鍵では、鍵を紛失したり、合鍵が返却されなかったりした場合、安全のために錠前装置を交換する必要があったが、本電子鍵システムによれば、電子鍵を格納した携帯電話を紛失したり、友人の携帯電話に発行した電子鍵が返却されなかったりしても、錠前装置側で電子鍵を無効化することが可能となり、ユーザの利便性を向上させることができる。

【発明を実施するための最良の形態】

【００１８】
以下、本発明の実施の形態を図面を参照して説明する。なお、本発明はこれら実施の形態に何ら限定されるものではなく、その要旨を逸脱しない範囲において、種々なる態様で実施し得る。
【００１９】
（本発明の概要）
図３１は、本発明の概要を示す図である。本発明では、認証要求装置３１０１が、認証装置３１０２により認証がされる。そのとき、認証のための情報が認証要求装置３１０１から認証装置３１０２へ送信される。
【００２０】
本発明の認証方法では原理的には、その情報が認証要求装置３１０１から認証装置３１０２へ送信される前に、認証装置３１０２から認証要求装置３１０１への情報の送信は必須ではない。ただし、認証要求装置３１０１と認証装置３１０２との間での同期を取ったり、成りすましによる攻撃を避けたりするなどのために、認証装置３１０２から認証要求装置３１０１へ情報が送信されてもよい。
【００２１】
図３２は、認証要求装置３１０１と認証装置３１０２との処理のシーケンス図を例示する。まず、ステップＳ３２０１において、認証要求装置は、暗号化第一情報と第二情報とを、認証装置へ向けて送信する。暗号化第一情報と第二情報とを受信した認証装置は、ステップＳ３２０２において、暗号化第一情報と第二情報との関係が所定の関係であるかどうかを判断する。もし、所定の関係であれば、認証要求装置は認証装置により認証される。その結果、例えば、認証要求装置のユーザに対して決済処理が行なわれたり、特定の場所への入場の許可が下されたり、鍵の開錠がされたりなどが行なわれる。
【００２２】
ここに、「暗号化第一情報」とは、認証装置が保持する復号鍵により復号化可能な暗号化形式で第一情報を暗号化した情報、あるいは、そのような情報を含む情報である。第一情報は、いかなる情報であってもよい。例えば、乱数、クレジットカード番号、電話番号、ＩＰアドレス、ユーザの指紋や虹彩などを記号化した生態認証情報、などでもよい。また、「第二情報」とは、第一情報との関係が所定の関係であるか判断することを目的とする情報である。例えば、第二情報は、第一情報と同じであるかどうかを判断することを目的とする情報であってもよい。また、第一情報と第二情報とが二進数で表わされたとき、第一情報と第二情報との差が所定の値になっているかどうかを判断することを目的とする情報であってもよい。
【００２３】
なお、本発明において、暗号化第一情報、第二情報としては、デジタル信号により表現可能な情報を念頭においている。したがって、本発明における認証要求装置と認証装置とは、デジタル計算機によって実現可能なものである。なお、デジタル計算機といってもデスクトップコンピュータのような移動が困難なもののみを想定しているものではなく、例えば、携帯電話、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｃｅ）などの可搬形ものも想定している。
【００２４】
図３３は、（１）暗号化第一情報、（２）第二情報、（３）第一情報と第二情報とが所定の関係にあるかどうかの判断の条件、の三つ組みの例を示す。
【００２５】
図３３（Ａ）においては、暗号化第一情報は、所定のパスワードを、認証装置が保持する復号鍵により復号化可能な形式で暗号化した情報（Ｅｎｃｒｙｐｔ（パスワード））であり、第二情報は、その所定のパスワードであり、判断の条件は、暗号化第一情報を、認証装置が保持する復号鍵により復号化して得られる情報（Ｄｅｃｒｙｐｔ（暗号化第一情報））が、第二情報と等しいかどうかどうかである。
【００２６】

暗号化第一情報がＥｎｃｒｙｐｔ（パスワード）であれば、Ｄｅｃｒｙｐｔ（暗号化第一情報）はパスワードになるので、第二情報がパスワードであれば、第二情報を入力した者は暗号化第一情報の内容を知っている者であることになる。したがって、第二情報を入力した者は、暗号化第一情報の正当な保持者となり認証が行なうことができる。

【００２７】

図３３（Ｂ）においては、暗号化第一情報は、Ｅｎｃｙｐｔ（パスワード）である。第二情報は、パスワードに所定の処理を加えて得られる情報（Ｆ（パスワード））である。「所定の処理」とは、認証要求装置と認証装置との間であらかじめ定められた処理を意味する。好ましくは、この所定の処理は、ＭＤ５（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ　５）やＳＨＡ１（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ　Ｖｅｒｓｉｏｎ１）などのように、それほど計算量を必要とせず、かつその逆関数を知ることが困難であるもの（このような処理は、不可逆演算あるいはハッシュ演算と呼ばれる場合がある）である。このような処理を用いることにより、第二情報からパスワードを知ることが困難にすることができる。

【００２８】

図３３（Ｂ）においては、所定の条件は、Ｆ（Ｄｅｃｒｙｐｔ（暗号化第一情報））と第二情報とが等しいかどうかとなる。なぜなら、暗号化第一情報がＥｎｃｒｙｐｔ（パスワード）であれば、Ｆ（Ｄｅｃｒｙｐｔ（暗号化第一情報））は、Ｆ（パスワード）となるからである。

【００２９】

なお、図３３（Ｂ）において、所定の処理（Ｆ）は、認証を行なうたびに変化するものであってもよい。例えば、認証要求装置と認証装置との間で時刻の同期を取っておき、現在時刻に応じて、Ｆが選択されてもよい。あるいは、認証要求装置から認証装置へ暗号化第一情報と第二情報が送信されることに先立って、認証装置から認証要求装置に対して乱数が送信され、その乱数により定まる処理であってもよい（例えば、入力された情報に乱数を連結（ＣＯＮＣＡＴＥＮＡＴＥ）し、その結果にＭＤ５やＳＨＡ１などの付加逆演算を行なう。）。

【００３０】

（実施の形態１）

図３４は、本発明の第１の実施の形態に係る認証要求装置の機能ブロック図を例示する。

【００３１】

認証要求装置３４００は、認証装置に対して認証を求める装置であって、暗号化第一情報取得部３４０１と、第二情報取得部３４０２と、送信部３４０３と、を有する。

【００３２】

「暗号化第一情報取得部」３４０１は、暗号化第一情報３４０４を取得する。例えば、キーボードなどの入力装置、フレキシブルディスク、光ディスク、ハードディスク、メモリカードなどの記録媒体より暗号化第一情報３４０４を取得する。

【００３３】

なお、暗号化第一情報３４０４は、図３５（Ａ）に示されるように、第一情報だけを暗号化したものであってもよい。あるいは、図３５（Ｂ）に示されるように、それは、第一情報に付加情報を付加して得られる情報を暗号化したものであってもよい。付加情報は、認証の目的によって決まるものであってもよい。例えば、暗号化第一情報が電子チケットを表わすものであれば、付加情報は、日時と座席番号を表わしていてもよい。

【００３４】

「第二情報取得部」３４０２は、第二情報３４０５を取得する。例えば、キーボードなどの入力装置、フレキシブルディスク、光ディスク、ハードディスク、メモリカードなどの記録媒体より第二情報３４０５を取得する。また、第二情報３４０５は、指紋や虹彩などの生態認証情報であってもよい。このような場合、第二情報取得部３４０２は、生態認証情報を取得するためのセンサーやカメラなどとなる。

【００３５】
「送信部」３４０３は、暗号化第一情報３４０１で取得した暗号化第一情報と、第二情報取得部で取得した第二情報とを関連付けて前記認証装置に対して送信する。「関連付けて」には、特別な意味は無いが、強いて挙げるとすれば、同時あるいは時間的に近接して、という意味であり、暗号化第一情報と第二情報とが分離できるように送信することである。送信は、有線によるもの、無線によるものを問わない。
【００３６】
図３６は、認証装置の機能ブロック図を例示する。
【００３７】
認証装置３６００は、受信部３６０１と、復号鍵保持部３６０２と、復号化部３６０３と、判断部３６０４と、を有する。
【００３８】
「受信部」３６０１は、認証要求装置の送信部から送信された暗号化第一情報と、その暗号化第一情報に関連付けて送信された第二情報とを受信する。暗号化第一情報と第二情報とが受信された後には、暗号化第一情報３６０５と第二情報３６０７とに分離される。
【００３９】
「復号鍵保持部」３６０２は、暗号化第一情報の復号化をするための復号鍵を保持する。復号鍵保持部３６０２は、第一情報が共有鍵により暗号化された場合には、その共有鍵を保持する。また、第一情報が公開鍵暗号方式により暗号化された場合、例えば、第一情報が公開鍵で暗号化された場合には、復号鍵保持部３６０２は、その公開鍵に対応する秘密鍵を保持する。なお、「保持」とは、ある程度の時間的な永続性があって、読み出し可能に記録することである。そのため、復号鍵保持部３６０２は、例えば、揮発性メモリ、不揮発性メモリ、ハードディスクなどにより実現される。また、耐タンパ性を持ったＩＣカードなどにより実現されてもよい。
【００４０】
「復号化部」３６０３は、受信部３６０１で受信した暗号化第一情報３６０５を復号鍵保持部３６０２に保持されている復号鍵を利用して復号化し第一情報３６０６を得る。すなわち、復号鍵を復号鍵保持部３６０２より読み出し、暗号化第一情報３６０５を復号化する。もし、暗号化第一情報３６０５が第一情報と付加情報とを暗号化したものであれば、復号化の結果より、第一情報を得る。
【００４１】
「判断部」３６０４は、復号化部３６０３で復号化した第一情報３６０６と、復号化前の第一情報である暗号化第一情報と関連付けられて受信された第二情報３６０７と、が所定の関係にあるか判断する。例えば、図３３に示された「判断の条件」が成立するかどうかを判断する。
【００４２】
図３７（Ａ）は、認証要求装置の処理のフロー図を例示し、図３７（Ｂ）は、認証装置の処理のフロー図を例示する。
【００４３】
認証要求装置は、ステップＳ３７０１において、暗号化第一情報取得部３４０１により、暗号化第一情報を取得する。
【００４４】
ステップＳ３７０２において、第二情報取得部３４０２により、第二情報を取得する。
【００４５】
ステップＳ３７０３において、送信部３４０３により、暗号化第一情報と第二情報とを送信する。
【００４６】
一方、認証装置は、ステップＳ３７０４において、受信部３６０１により、暗号化第一情報と第二情報とを受信する。
【００４７】

ステップＳ３７０５において、復号化部３６０３により、復号鍵を取得し、ステップＳ３７０６において、暗号化第一情報を、復号鍵を用いて復号化し、第一情報を得る。

【００４８】

ステップＳ３７０７において、判断部３６０４により、第一情報と第二情報とが所定の関係にあるかどうかを判断する。

【００４９】

なお、図３７に示したフロー図は処理の一例であって、例えば、ステップＳ３７０１とステップＳ３７０４の前に、認証要求装置と認証装置との間での同期の処理や、認証装置から認証要求装置へ何らかの情報が送信されるようになっていてもよい。

【００５０】

本実施の形態によれば、認証要求装置側に暗号鍵などの秘密情報を格納しておく必要がなく、また、暗号化を行なう処理も必須ではない認証のための装置及び方法が提供される。

【００５１】

（実施の形態２）

図３８は、本発明の第２の実施の形態に係る認証要求装置の機能ブロック図を例示する。

【００５２】

認証要求装置３８００の構成は、第１の実施の形態に係る認証要求装置が、暗号化第一情報保持部３８０１を有する構成となっている。

【００５３】

「暗号化第一情報保持部」３８０１は、暗号化第一情報を保持する。例えば、暗号化第一情報を、メモリ、磁気ディスク、光ディスクなどにより保持する。

【００５４】

本実施の形態においては、暗号化第一情報取得部３４０１は、暗号化第一情報保持部３８０１にて保持されている暗号化第一情報を取得する。したがって、認証要求装置３８００の動作は、図３７（Ａ）に例示したフロー図において、Ｓ３７０１においては、暗号化第一情報は暗号化第一情報保持部３８０１より取得されることになる。

【００５５】

本実施の形態によれば、暗号化第一情報が暗号化第一情報保持部３８０１にて保持されているため、認証要求装置３８００が認証装置により認証された場合、認証要求装置３８００に第二情報を入力した者を認証することができる。

【００５６】

（実施の形態３）

図３９は、本発明の第３の実施の形態に係る認証要求装置の機能ブロック図を例示する。

【００５７】

認証要求装置３９００の構成は、第１または第２の実施の形態に係る認証要求装置が、認証情報入力部３９０１と、認証情報加工部３９０２と、を有している構成となっている。

【００５８】

「認証情報入力部」３９０１は、認証を目的とした情報である認証情報を入力するための部である。例えば、あらかじめ定められたパスワードや暗証番号を入力するための部であり、例えば、キーボードやテンキーである。あるいは、指紋や虹彩などの生態認証情報を取得するためのセンサーやカメラであってもよい。

【００５９】

「認証情報加工部」３９０２は、認証情報入力部３９０１から入力された認証情報を加工する。「加工する」とは、何らかの演算を施すことである。例えば、他の情報と連接する演算を行なったり、ＭＤ５やＳＨＡ１などのハッシュ関数のアルゴリズムに基づいた演算を行なったりする。

【００６０】
本実施の形態においては、第二情報は、認証情報加工部３９０２にて加工された情報となる。したがって、第二情報取得部３４０２は、認証情報加工部３９０２で加工された情報を第二情報として取得することになる。
【００６１】
認証情報加工部３９０２での認証情報の加工の処理は、任意のものが使用できる。また、毎回同じ加工がされ、同じ認証情報に対して同じ第二情報が得られる必要はなく、認証情報が加工されるたびに、異なる第二情報が得られるようになっていてもよい。このように毎回異なる加工がされることにより、送信部３４０３から送信される第二情報が盗聴などされても安全性を高めることができる。
【００６２】
なお、このように毎回異なる加工がされても認証が行なえるようにするためには、認証を行なう認証装置側で、認証情報加工部３９０２でどのような加工が行なわれるかを認識する必要がある。このため、例えば、認証に先立って認証装置と認証要求装置との間で、どのような加工が行なわれるかの同期の処理が必要となる。例えば、加工のアルゴリズムを前もっていくつか用意しておき、認証要求装置から、何番目のアルゴリズムを用いて認証情報が加工されたかが認証装置へ送信されるようになっていてもよい。あるいは、認証装置から何番目のアルゴリズムを用いて認証情報を加工するべきかが認証要求装置へ送信されるようになっていてもよい。あるいは、認証装置と認証要求装置との間で時刻を同期させておき、時刻に応じてアルゴリズムが選択されるようになっていてもよい。
【００６３】
加工のアルゴリズムを変えずに、アルゴリズムのパラメータを変更するようになっていてもよい。例えば、認証情報に別の情報を連接して、その結果に対してハッシュ関数を施す加工を行なう場合には、別の情報をパラメータとして毎回変化するようにしてもよい。このために、認証要求装置と認証装置との間で、そのパラメータを共有するようにする。例えば、認証要求装置から認証装置へパラメータを送信したり、認証装置から認証要求装置へパラメータを送信したり、あるいは、認証要求装置と認証装置との間で時刻を同期させておき、時刻に応じてパラメータが決定されるようになっていてもよい。
【００６４】
図４０（Ａ）は、本実施の形態に係る認証要求装置の処理のフロー図を例示する。ステップＳ４００１において、暗号化第一情報取得部３４０１により暗号化第一情報を取得する。例えば、認証要求装置の外部から取得したり、暗号化第一情報保持部３８０１がある場合には、そこから取得したりする。
【００６５】
ステップＳ４００２において、認証情報入力部３９０１により、認証情報を入力する。
【００６６】
ステップＳ４００３において、認証情報加工部３９０２により、認証情報を加工して第二情報とする。
【００６７】
ステップＳ４００４において、送信部３４０３により、暗号化第一情報と第二情報とを送信する。
【００６８】
図４０（Ｂ）は、本実施の形態に係る認証装置の処理のフロー図を例示する。ステップＳ４００５において、暗号化第一情報と第二情報とを受信する。
【００６９】
ステップＳ４００６において、復号鍵を取得する。
【００７０】
ステップＳ４００７において、暗号化第一情報を復号鍵を用いて復号化し、第一情報を得る。
【００７１】

ステップＳ４００８において、第一情報を加工する。ここの加工は、ステップＳ４００３で認証情報が加工されたのと同じアルゴリズムを用いて行ない、また、必要ならば、認証要求装置での認証情報の加工に用いられたのと同じパラメータを用いて行なう。

【００７２】

ステップＳ４００９において、加工された第一情報と第二情報が所定の関係にあるかどうかを判断する。「所定の関係」の一例として、同一であるという関係がある。

【００７３】

本実施の形態によれば、認証情報が加工されて得られる第二情報が送信されるため、例えば認証情報の加工のアルゴリズムを秘密のものにしておくことにより、第二情報より認証情報を推測されにくくすることができる。また、ハッシュ関数を用いて加工することにより、認証情報の加工のアルゴリズムが秘密のものでなくなっても第二情報より認証情報を知ることが困難であるので、安全性を高めることができる。また、ハッシュ関数の処理は一般の暗号化の処理よりも要求される計算量が少ないので、認証要求装置の簡略化、コストダウン、処理の高速化を図ることができる。

【００７４】

（実施の形態４）

本発明の第４の実施の形態として、情報関連付装置を説明する。情報関連付装置とは、暗号化第一情報を生成するための装置である。

【００７５】

図４１は、情報関連付装置の機能ブロック図を例示する。情報関連付装置は、認証情報取得部４１０１と、第一情報生成部４１０２と、暗号鍵保持部４１０３と、暗号化部４１０４と、を有する。

【００７６】

「認証情報取得部」４１０１は、認証情報を取得する。例えば、キーボード、テンキー、あるいは、メモリカードなどの媒体より取得する。あるいは、虹彩、指紋などの生態認証情報を取得するカメラやセンサーなどにより取得してもよい。あるいは、ネットワークを経由して離れた場所などから送信される認証情報を取得してもよい。この場合、ネットワークを経由して行なわれる通信は、例えばＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）などにより、暗号化されているのが望ましい。

【００７７】

「第一情報生成部」４１０２は、認証情報取得部で取得した認証情報を利用して前記認証情報と、所定の関係を有するように第一情報を生成する。例えば、認証情報をそのまま第一情報としてもよいし、認証情報に所定の演算処理を行なって第一情報を生成するようにしてもよい。

【００７８】

「暗号鍵保持部」４１０３は、暗号化の鍵を保持する。例えば、メモリやハードディスクなどに鍵を保持する。この暗号化の鍵は、共通鍵暗号化方式に用いられる鍵であってもよいし、公開鍵暗号化方式に用いられる鍵（例えば、秘密鍵に対応する公開鍵）であってもよい。

【００７９】

「暗号化部」４１０４は、第一情報生成部４１０４で生成された第一情報を暗号鍵保持部４１０３で保持された暗号化の鍵で暗号化する。

【００８０】

図４２は、情報関連付装置の処理のフロー図を例示する。ステップＳ４２０１において、認証情報取得部４１０１により、認証情報を取得する。

【００８１】

ステップＳ４２０２において、第一情報生成部４１０２により、第一情報を生成する。

【００８２】

ステップＳ４２０３において、暗号化部４１０４により、暗号化の鍵を取得し、ステップＳ４２０４において、第一情報を暗号化の鍵で暗号化する。

【００８３】
その後、暗号化された第一情報は、暗号化第一情報として、メモリカードの媒体に記録されたり、認証要求装置に保持されたりする。

【００８４】
本実施の形態により、暗号化第一情報を生成することができる。特に、認証装置と異なる装置で暗号化第一情報が生成できるので、認証装置と情報関連付装置とがネットワークなどで通信可能になっていることは必須ではなくなる。これにより認証装置を簡略化、小型化などすることができる。

【００８５】
（実施例）
図４３は、これまで説明した実施の形態の実施例を例示する。

【００８６】
図４３には、認証要求装置４３０１と認証装置４３０２が図示されている。認証要求装置４３０１は、不揮発性メモリ４３０３を備えている。不揮発性メモリ４３０３は取り外しが可能なものであってもよいし、取り外しが不可能なものであってもよい。不揮発性メモリ４３０３は、Ｖ＿Ａｕｔｈを暗号化したものを保持している。Ｖ＿Ａｕｔｈは第一情報に相当し、Ｖ＿Ａｕｔｈを暗号化したものが暗号化第一情報に相当する。また、不揮発性メモリ４３０３はユーザＩＤを保持していてもよい。ユーザＩＤは、Ｖ＿Ａｕｔｈを暗号化した時間、ユーザの持つクレジットカード番号などのように、同一の値が得られる確率がそれほど大きくない値である。ユーザＩＤを使用する目的の一つは、Ｖ＿Ａｕｔｈを生成する際に、パスワードが他のＶ＿Ａｕｔｈの生成時と同じになってしまい、同じＶ＿Ａｕｔｈが生成されることを防ぐことにある。また、暗号化第一情報が、何のための情報であるかを示すものであってもよい。

【００８７】
Ｖ＿Ａｕｔｈは、図４４の一行目に示される式に基づいて生成される。ここに「パスワード」は所定の認証情報であり、「｜｜」は連結の演算を表わし、「パスワード｜｜ユーザＩＤ」により、パスワードにユーザＩＤを連結して得られる情報を表わす。$Hash_1$は、ハッシュ関数である。

【００８８】
認証要求装置４３０１が認証装置４３０２に対して認証を求める際には、（１）認証情報が入力される。この入力は、認証要求装置のユーザにより認証情報入力部を用いて行なわれる。例えば、キーボードやテンキーで入力が行なわれたり、ユーザの指紋や虹彩などの生態認証情報の入力が行なわれたりする。

【００８９】
（２）から（４）までが認証情報加工部の処理であり、（２）Ｖ＿Ａｕｔｈ´を、図４４の（２）に示した式に基づいて求める。次に、（３）チャレンジを認証装置４３０２より受信する。「チャレンジ」とは、必要に応じて生成される値である。望ましくは、認証装置が送信するたびに異なる値が生成され、次に生成される値を予測することが困難な値である。Ｖ＿Ａｕｔｈ´が求まりチャレンジが受信されると、（４）Ｕ＿Ａｕｔｈ´を計算する。Ｕ＿Ａｕｔｈ´は、図４４の（４）に示した式に基づいて求められる。$Hash_2$は、ハッシュ関数であり、$Hash_1$と同じ関数であってもよいし、別の関数であってもよい。

【００９０】
Ｕ＿Ａｕｔｈ´が求められると、（５）不揮発性メモリに格納されたＶ＿Ａｕｔｈを暗号化されたものを取り出し、関連付けを行ない、（６）認証装置４３０２へ送信する。

【００９１】
以後、認証装置４３０２の処理となり、認証装置の不揮発性メモリなどに保持されている復号鍵を取得し、（７）受信したＶ＿Ａｕｔｈを暗号化したものの復号化を行ない、Ｖ＿Ａｕｔｈを得る。次に、（８）Ｖ＿Ａｕｔｈと、認証要求装置へ送信されたチャレンジと、から図４４の（８）の式に基づいてＵ＿Ａｕｔｈを計算する。最後に（９）Ｕ＿Ａｕ

ｔｈとU__Ａｕｔｈ´との照合を行なう。もし、認証要求装置に入力された認証情報がＶ__Ａｕｔｈを生成したときのパスワードと等しい時には、U__ＡｕｔｈとU__Ａｕｔｈ´は等しくなるので、これにより、認証情報を入力したユーザがＶ__Ａｕｔｈを暗号化したものの発行を受けた者であるかを認証することができる。

【００９２】

認証要求装置では、認証情報の加工に使われる演算は、連結とハッシュ関数であるので、要求される計算量は大きくなく、認証要求装置の小型化、コストダウンなどを図ることができる。また、チャレンジを用いて認証情報の加工が行なわれるので、認証要求装置から認証装置へ送信される情報が知られてもセキュリティの問題が発生しにくい。また、認証装置の側には、従来の認証方法と異なり、ユーザＩＤ、パスワードを保持しておく必要がない。このため、Ｖ__Ａｕｔｈを暗号化されたものの発行に制限が課せられることはない。

【００９３】

（実施の形態５）

本発明の第５の実施の形態として、電子クレジット決済システムについて説明する。図３０は、本実施の形態５における電子クレジット決済システムのブロック構成図を示している。この電子クレジット決済システムは、ユーザが所有する携帯電話１と、クレジットカード会社のセンター２と、小売販売店に設置されるクレジット決済端末３とによって構成され、携帯電話１とセンター２とは、携帯電話の無線通信ネットワーク４によって接続され、クレジット決済端末３とセンター２とはクレジット決済ネットワーク５によって接続され、携帯電話１とクレジット決済端末３とは、ローカルワイヤレス通信機能（赤外線通信、Bluetooth、無線ＬＡＮ、非接触ＩＣカードの無線通信など）６を用いて、アドホックに通信する。携帯電話１には、予め、Ｊａｖａ（登録商標）クレジット決済アプリがダウンロードされている。また、クレジット決済端末３には、電子クレジットに施されたクレジットカード会社による電子署名を検証するため、クレジットカード会社の証明書が格納され、センター２とクレジット決済端末３には、電子クレジットの暗号鍵を生成するためのマスター鍵Kmか管理されている。

【００９４】

まず、携帯電話１には、ユーザが所有するクレジットカードに対応する電子クレジット（電子情報化したクレジットカード、電子バリューの一種）をセンター２からダウンロードする。図１は、電子クレジットのダウンロードの手順を示している。まず、ユーザがＪａｖａ（登録商標）クレジット決済アプリを起動(100)すると、メニュー画面が表示され(101)、ユーザが電子クレジット発行要求操作(102)を行うと、クレジットカードのカード番号とPIN、さらに、ダウンロードする電子クレジットに対応するパスワード(VPW)を入力する画面が表示される(103)。ユーザがカード番号とPIN、及び、パスワードを入力すると(104)、携帯電話１は、パスワード(VPW)のハッシュ演算結果 Hash(VPW)をパスワードの参照データとして携帯電話１のメモリに格納し(105)、さらに、カード番号(CN)と時刻(T)とから、ユーザ識別情報 UID = Hash(CN || T)（※ ||はデータの連結を示す）を生成してメモリに格納し(106)、さらに、パスワード(VPW)とユーザ識別情報(UID)とから、バリュー認証情報 F(VPW) = Hash(VPW || UID) を生成し(107)、カード番号とPINとバリュー認証情報 F(VPW)とを含む、電子クレジット発行要求をセンター２に送信する（108）。センター２は、カード番号とPINとから、クレジットカードの所有者であるかユーザを認証し(109)、認証された場合に、電子クレジットの中にバリュー認証情報 F(VPW)を埋め込んで電子クレジット(ev)を生成する(110)。さらに、バリュー認証情報 F(VPW)のハッシュ演算し、マスター鍵Kmと連結して、さらに、ハッシュ演算して、電子クレジット(ev)を暗号化する共通鍵暗号方式の暗号鍵Kc = Hash(Km || Hash(F(VPW)))を生成する(111)。生成した暗号鍵Kcを用いて、電子クレジット(ev)を暗号化して、暗号化された電子クレジットencrypt(ev) = Enc(Kc, ev) を生成する(112)。暗号化された電子クレジットencrypt(ev)は、携帯電話１に送信され(113)、暗号化された電子クレジットencrypt(ev)は、携帯電話のメモリに格納され(114)、携帯電話１がダウンロードの完了を表示して、電子クレジット

のダウンロード処理を完了する。

【００９５】

暗号化された電子クレジット300のデータ構造は、図３に示すようになっており、暗号化される前の電子クレジットは、クレジットカードのカード番号、有効期限、ユーザ名、発行者名等を示す電子クレジット情報 301と、電子クレジット情報 301の部分に対するクレジットカード会社による電子署名302と、バリュー認証情報 F(VPW)303とから構成されている。

【００９６】

Ｊａｖａ（登録商標）クレジット決済アプリを終了すると、ユーザが入力したパスワードはメモリから消去される。携帯電話のメモリに保持されているデータは、パスワードをハッシュ演算したものなので、仮に、携帯電話が第三者に盗まれて、内部のメモリが解析されたとしても、パスワードが知られる心配が無い。

【００９７】

次に、ダウンロードした電子クレジットを用いて、クレジット決済を行う手順について、図２を用いて説明する。クレジット決済端末３がチャレンジ情報として乱数Rを生成する。ユーザがＪａｖａ（登録商標）クレジット決済アプリを起動(201)すると、メニュー画面が表示され(202)、ユーザが電子クレジット決済操作(203)を行うと、電子クレジットに対応するパスワード(VPW)を入力する画面が表示される(204)。ユーザがパスワード(VPW')を入力すると(205)、携帯電話１は、パスワード(VPW')のハッシュHash(VPW')を計算し、メモリに格納された参照データのHash(VPW)と照合してユーザを認証する(206)。参照データと一致しなかった場合にはエラーを表示し（図には記載していない）、参照データと一致した場合には、クレジット決済端末３からの電子クレジット要求を受信する(207)。電子クレジット要求には、乱数Rが含まれており、携帯電話１は、ユーザが入力したパスワード(VPW')を用いて、バリュー認証情報 F(VPW')= Hash(VPW'|| UID) 及び 、バリュー認証情報 F(VPW')と乱数Rとの連結のハッシュ Hash(F(VPW') || R)、バリュー認証情報のハッシュ Hash(F(VPW'))をそれぞれ計算し(208)、クレジット決済端末３に電子クレジットとして、暗号化された電子クレジット encrypt(ev)と共に、Hash(F(VPW') || R)と、Hash(F(VPW')) とを送信する (209) 。クレジット決済端末３は、受信したバリュー認証情報のハッシュ Hash(F(VPW'))とマスター鍵Kmとから、その連結のハッシュを計算し、暗号化された電子クレジットの共通鍵暗号方式の復号鍵Kc'= Hash(Km || Hash(F(VPW'))) を生成し、電子クレジットの暗号を復号化する(210)。クレジット決済端末３は、復号化した電子クレジット(ev)からバリュー認証情報F(VPW)を取り出し、乱数Rとの連結のハッシュ Hash(F(VPW) || R)を計算し、携帯電話１から受信したHash(F(VPW') || R)と照合し、一致していた場合、ユーザが電子クレジットの正しい所有者であると認証する(211)。一致しなかった場合には、ユーザに対して、エラーを示す（図には記載してない）。さらに、クレジット決済端末３は、電子署名302を検証し(212)、エラーが検出された場合には、ユーザに対して、エラーを示す。電子署名302の検証(212)において、エラーが検出されなかった場合には、クレジット決済端末３は、携帯電話１に認証結果を送信し(213)、さらに、センター２にクレジット決済の承認要求を送信し(215)、センター２が承認処理を行い(216)、センター２からクレジット決済端末３に承認要求応答が送信されて(217)、クレジット決済端末３でのクレジット決済処理は完了する。一方、認証結果を受信した携帯電話１は、完了を表示して(214)、電子クレジットのクレジット決済処理を完了する。この場合も、Ｊａｖａ（登録商標）クレジット決済アプリを終了すると、ユーザが入力したパスワードはメモリから消去される。

【００９８】

携帯電話１とクレジット決済端末３との間で交換されるデータは、すべて、ハッシュ演算、または、暗号化されたデータであるため、仮に、第三者によって携帯電話１とクレジット決済端末３との間の通信が盗聴されたとしても、その盗聴したデータを用いて、成りすましを行うことは出来ない。

【００９９】

以上の説明では、電子クレジットに対応する認証情報をパスワードとしたが、ユーザの指紋や虹彩などの生態情報としても良い。この場合、携帯電話１は、指紋認証センサーや虹彩認証カメラなどの機能を備える。

【０１００】

また、本実施の形態５では、電子クレジット決済システムについて述べたが、電子クレジットの電子クレジット情報301の部分の内容を変更することで、同様の認証メカニズムを電子デビット決済システムや、電子チケットシステム、電子クーポンシステム、または、会員証やＩＤカードなど、他の電子バリューの認証処理にも用いることができる。例えば、電子デビット決済システムの場合には、電子クレジット情報301の部分に、銀行口座番号、ユーザ名、発行者名などの情報を入れるだけでよい。

【０１０１】

（実施の形態６）

次に、本発明の第６の実施の形態として、複数種類のクレジットカード及び複数のアクワイアラに対応する携帯型のクレジット決済端末を用いる電子クレジット決済システムについて説明する。本実施の形態６では、電子情報化したクレジットカードである電子クレジット（ev：電子バリューの一種）を、複数種類、携帯電話で管理し、ユーザが選択した電子クレジット(ev)を用いて、携帯型のクレジット決済端末との間で決済が行われる。クレジット決済端末が携帯型であるため、例えば、小売店や飲食店などの加盟店の店員がクレジット決済端末を持ち歩くことができ、お客さん（ユーザ）を待たせることなく、売り場やフロアーなどの接客の現場で決済を行うことができる。

【０１０２】

図４は、本実施の形態６における電子クレジット決済システムのブロック構成図を示している。この電子クレジット決済システムは、ユーザが所有する携帯電話401と、クレジットカード会社のセンター402と、加盟店の店員が持つクレジット決済端末403と、加盟店に対してクレジット決済サービスを提供するアクワイアラ404と、携帯電話401とセンター402との間を結ぶネットワーク405と、クレジット決済端末403とアクワイアラ404との間を結ぶネットワーク406とによって構成される。

【０１０３】

ネットワーク405は、携帯電話の無線通信ネットワークとインターネットによって構成され、携帯電話401とセンター402との無線通信による通信を可能にする。携帯電話401とセンター402との通信では、常に、SSL(Secure Sockets Layer)やTLS(Transport Layer Security)などのセキュアセッションを確立され、通信データは暗号化されて伝送される。

【０１０４】

ネットワーク406は、無線通信ネットワークとクレジット決済ネットワークによって構成され、クレジット決済端末403とアクワイアラ404との無線通信による通信を可能にする。携帯電話401とクレジット決済端末403とは、ローカルワイヤレス通信機能（赤外線通信、Bluetooth、無線ＬＡＮ、非接触ＩＣカードの無線通信など）を用いて、アドホックに接続して通信する。センター402とアクワイアラ404とは、専用線を用いて通信する。

【０１０５】

クレジット決済端末403は、複数種類の電子クレジットの決済に対応し、アクワイアラが異なる場合にも対応する。したがって、図４では、センターとアクワイアラは、１つずつしか図示していないが、実際にはクレジット決済端末403は、ネットワーク406を介して複数のアクワイアラと接続し、複数のクレジットカード会社のセンターとの間でクレジット決済処理を行う。

【０１０６】

携帯電話401には、予め、電子クレジット(ev)を管理するワレットアプリケーションがダウンロードされている。また、クレジット決済端末403には、複数種類のクレジットカードの決済に対応するため、カード種別毎にカード情報が格納され、センター402とクレジット決済端末403には、電子クレジット(ev)の暗号化されている部分を復号化する暗号鍵を生成するためのマスター鍵(Km)か管理されている。

【０１０７】
図５は、クレジット決済端末403の内部構成を示すブロック図である。クレジット決済端末403は、ＲＯＭ(Read Only Memory)502に格納されたプログラムにしたがって、ＥＥＰＲＯＭ(Electrically Erasable Programmable ROM)503に格納されたデータの処理と送受信データの処理、並びにバス513を介して他の構成要素の制御を行なうＣＰＵ(Central Processing Unit)500と、ＬＣＤ505と、ローカルワイヤレス通信Ｉ／Ｆ510と、セキュリティカードスロット501と、クレジット決済端末を操作するスイッチ508と、スイッチ操作を検出するキー制御部509と、スピーカ506をドライブする音声処理部507と、アンテナ512を介して行う無線データ通信を制御する無線通信部511と、セキュリティカード501とによって構成される。
【０１０８】
ローカルワイヤレス通信Ｉ／Ｆ510は、赤外線通信や、Bluetooth、無線ＬＡＮ、非接触ＩＣカードの無線通信などの通信Ｉ／Ｆであり、携帯電話とアドホックに接続して通信を行うためのものである。
【０１０９】
セキュリティカード501は、マスター鍵(Km)を安全に管理し、電子クレジットの認証処理を安全に行うためのデバイスであり、ＴＲＭ部（Tamper Resistant Module）514と、フラッシュメモリ部515とによって構成される。ＴＲＭ部514は、さらに、ＣＰＵ516と、ＲＯＭ517と、ＲＡＭ518と、ＥＥＰＲＯＭ519と、コ・プロセッサ520によって構成され、外部からの不正なアクセスを防止する耐タンパ機能を有している。
【０１１０】
フラッシュメモリ部515には、図６に示すように、電子クレジット情報リスト601と決済履歴情報602とが、それぞれ暗号化されて格納されている。電子クレジット情報リスト601は、クレジット決済端末が対応する種類の電子クレジットに関する情報が登録されたリストであり、決済履歴情報602は、クレジット決済端末が行った電子クレジット決済の履歴情報である。電子クレジット情報リスト601と決済履歴情報602の暗号化及び復号化は、ＣＰＵ516がコ・プロセッサ520を制御して行う。
【０１１１】
図６は、電子クレジット情報リスト601に４種類の電子クレジット(ev)に関する情報が登録されている場合を示している。電子クレジット情報リスト601には、１つの種類の電子クレジット(ev)に対し、カード種別、マスター鍵(Km)、クレジットカード会社証明書、ネガリスト、アクワイアラ情報、リスク管理情報がそれぞれ登録されている。
【０１１２】
カード種別は、電子クレジット(ev)の種類を示す識別情報であり、マスター鍵(Km)は、この種類の電子クレジット(ev)の暗号化されている部分を復号化する暗号鍵を生成するためのマスター鍵、クレジットカード会社証明書は、この種類の電子クレジット(ev)を発行しているクレジットカード会社の証明書、ネガリストは、この種類の電子クレジット(ev)に関し無効になった電子クレジット(ev)のカード番号（識別情報）のリスト、アクワイアラ情報は、この種類の電子クレジット(ev)に関するクレジット決済サービスを提供するアクワイアラに関する情報、リスク管理情報は、この種類の電子クレジット(ev)において決済処理を行う場合のフロアーリミットなどのオンライン認証を行うか否か等を判定する際に用いる情報である。
【０１１３】
この他、電子クレジット情報リスト601には、電子クレジット(ev)の種類ごとに電子クレジット決済処理の際に用いる効果音などの音声情報や画像情報などのマルチメディア情報が登録されていても良い。例えば、その電子クレジット(ev)の種類またはクレジットカードブランドに固有の音声情報や画像情報を登録し、決済処理が完了した際にその効果音をスピーカから出力し、画像情報をＬＣＤに表示するようにすることで、その種類（またはクレジットカードブランド）の電子クレジット(ev)が使用されたことを明示的に示すことができる。

【０１１４】
フラッシュメモリ部515に格納されている情報へのアクセスは、セキュリティカード501のＣＰＵ516によって制御されており、クレジット決済端末403は、セキュリティカード501のＴＲＭ部514を介して、決済履歴情報602への書込みと読出しを行うことは出来るが、電子クレジット情報リスト601は読出しのみで、書込みを行うことは出来ない。また、電子クレジット情報リスト601の中でも、マスター鍵(Km)は、クレジット決済端末403からは読出しも書込みも出来ないように制御されている。

【０１１５】
電子クレジット情報リスト601は、セキュリティカード501とアクワイアラとが、クレジット決済端末403及びネットワーク406を介し、暗号化された通信セッションを確立して、必要に応じて更新される。例えば、加盟店とアクワイアラとの契約に基づき、電子クレジット情報の追加や削除、リスク管理情報の更新が行われ、また、安全性を高めるために、マスター鍵(Km)やネガリストの更新が行われる。

【０１１６】
携帯電話401は、ローカルワイヤレス通信Ｉ／Ｆを備えており、携帯電話401のワレットアプリケーションは、ローカルワイヤレス通信Ｉ／Ｆを介してクレジット決済端末403とアドホックに接続し、ワレットアプリケーションが管理している電子クレジット(ev)を用いて電子クレジット決済を行う。

【０１１７】
携帯電話401のメモリ（不揮発性メモリ）には、ワレットアプリケーションが管理する情報として、図７に示すように、ワレット表示情報701、ワレット音声情報702、電子クレジットリスト703が格納されている。ワレット表示情報701は、ワレットアプリケーションが携帯電話に表示する画面に用いる画像や映像情報などの表示情報であり、ワレット音声情報702は、ワレットアプリケーションが使用する効果音やメロディ情報などの音声情報、電子クレジットリスト703は、ワレットアプリケーションが管理している電子クレジット(ev)のリストである。

【０１１８】
図７は、電子クレジットリスト703に３つの電子クレジット(ev)が登録されている場合を示している。電子クレジットリスト703には、１つの電子クレジット(ev)に対し、参照データ、ユーザ識別情報(UID)、電子クレジット(ev)、プロパティがそれぞれ登録されている。参照データとユーザ識別情報(UID)については、後で詳しく説明する。プロパティは、その電子クレジット(ev)に設定された属性情報であり、例えば、ワレットアプリケーションが電子クレジットの一覧を表示する際の順番や、電子クレジット決済の際に使用される効果音や、ＬＥＤやバイブレータなどの動作が設定されている。例えばユーザは、利用頻度に応じて電子クレジットが表示される順番を設定したり、電子クレジット決済が完了した時、または、決済が失敗した時に出力される音をワレット音声情報702からそれぞれ選択して設定したり、電子クレジット決済が完了した時にＬＥＤを点滅させたり、決済が失敗した時にバイブレータを動作させたりといった設定を選択的に行うことができる。

【０１１９】
図８は、電子クレジット(ev)のデータ構造を示している。電子クレジットは、大きく分けて、電子クレジット公開情報801とセキュリティ情報800と表示用情報805とから構成される。セキュリティ情報800は、電子クレジットの認証処理に用いる情報であり、マスター鍵(Km)から生成される暗号鍵によって暗号化されている。また、表示用情報805は、ワレットアプリケーションが電子クレジットを画面に表示する際に使用するクレジットカードのロゴマークやユーザの写真、レイアウト情報などの表示情報であり、オプションで設定される。したがって、電子クレジット(ev)によって、表示用情報805を持つものと、持たないものとがある。

【０１２０】
電子クレジット公開情報801は、電子クレジットのカード種別、カード番号、有効期限、ユーザ名、発行者名等の電子クレジットに関するユーザに公開すべき情報が記述されて

いる部分で、ワレットアプリケーションは、電子クレジットを画面に表示する際にこの電子クレジット公開情報801を使用する。

【０１２１】

セキュリティ情報800は、さらに、電子クレジット秘密情報802と、バリュー認証情報803と署名情報804とから構成される。バリュー認証情報803については、後で詳しく説明する。

【０１２２】

電子クレジット秘密情報802は、クレジットカード会社が設定したリスク管理情報等の電子クレジットに関するユーザに必ずしも公開する必要のない情報が記述されている部分で、電子クレジット決済の際に、クレジット決済端末403側で暗号が復号化され、オンライン認証を行うか否か等の判定に用いられる情報である。

【０１２３】

署名情報804は、電子クレジット公開情報801と、暗号化する前の電子クレジット秘密情報802及びバリュー認証情報803とを連結したデータに対するクレジットカード会社による電子署名であり、電子クレジット決済の際に、クレジット決済端末403側で暗号が復号化され、電子署名を検証することによって、電子クレジット(ev)の有効性の検証に用いられる。

【０１２４】

署名情報804は、公開鍵暗号方式に基づく、安全性上、充分な鍵長の鍵を用いて生成された電子署名であることが望ましいが、クレジットカード会社の判断で、電子クレジット公開情報801と、暗号化する前の電子クレジット秘密情報802及びバリュー認証情報803とを連結したデータに対するハッシュ演算の結果であっても良い。

【０１２５】

次に、まず、ユーザがセンター402から携帯電話401に電子クレジット(ev)をダウンロードする手順について説明する。図９は、電子クレジット(ev)のダウンロードの手順を示している。まず、ユーザがワレットアプリケーションを起動(900)すると、メニュー画面が表示され(901)、ユーザがメニュー選択によって電子クレジット発行要求操作(902)を行うと、電子クレジットのカード番号とPIN(Personal Identification Number)、さらに、ダウンロードする電子クレジット(ev)に対応してユーザが設定するバリューパスワード(VPW：value password)を入力する画面が表示される(903)。この場合のカード番号とPINは、ユーザが既に所有しているクレジットカードのカード番号とPINであり、ダウンロードする電子クレジットは、その子カードという位置付けになる。また、子カードという位置付けではなく、ユーザとクレジットカード会社との新たな契約として電子クレジットを発行しても良い。この場合、ユーザにはクレジットカード会社から郵送等で、電子クレジットのための専用のカード番号及びPINが知らされている。

【０１２６】

ユーザがカード番号とPIN、及び、バリューパスワードを入力すると(904)、携帯電話401は、バリューパスワード(VPW)のハッシュ演算結果 Hash(VPW)をバリューパスワードの参照データとして携帯電話401のメモリに格納し(905)、さらに、カード番号(CN)と時刻(T)とから、ユーザ識別情報 UID = Hash(CN || T) (※ ||はデータの連結を示す) を生成してメモリに格納し(906)、カード番号(CN)とPINとユーザ識別情報(UID)とバリューパスワード(VPW)を含む電子クレジット発行要求をセンター402に送信する(907) 。この時、参照データHash(VPW)とユーザ識別情報 UID = Hash(CN || T)は、携帯電話401のメモリ上の電子クレジットリスト703に、新たにダウンロードする電子クレジットに関するデータとして、参照データとユーザ識別情報のフィールドにそれぞれ格納される。

【０１２７】

電子クレジット発行要求を受信したセンター402は、カード番号(CN)とPINとから、発行する電子クレジットの所有者となるべきユーザであるかユーザを認証し(908)、認証された場合、センター402では、バリューパスワード(VPW)とユーザ識別情報(UID)とから、バリュー認証情報 F(VPW) = Hash(VPW || UID) を生成し(909)、バリュー認証情報 F(VPW)

をハッシュ演算し、マスター鍵Kmと連結して、さらに、ハッシュ演算をして、電子クレジット(ev)を暗号化する共通鍵暗号方式の暗号鍵Kc = Hash(Km || Hash(F(VPW)))を生成する(910)。さらに、センター402は、電子クレジット(ev)の電子クレジット公開情報を生成し、ユーザの信用情報とバリューパスワード(VPW)のリスク評価の結果とに基づいて電子クレジット秘密情報を生成し、生成したバリュー認証情報 F(VPW)と暗号鍵Kcとを用いて、図８に示したデータ構造を持つ電子クレジット(ev)を生成する(911)。この時、カード番号(CN)とPINから、ユーザが認証されなかった場合には、エラーメッセージがセンター402から携帯電話401に送られ、電子クレジット(ev)のダウンロードの処理を終了する（図には記載していない）。

【０１２８】

生成された電子クレジット(ev)は、携帯電話401に送信され(912)、電子クレジット(ev)は、携帯電話のメモリに格納され(913)、携帯電話401がダウンロードの完了を表示して(914)、電子クレジットのダウンロード処理を完了する。この時、電子クレジット(ev)は、携帯電話401のメモリ上の電子クレジットリスト703に、新しい電子クレジットとして格納される。また、プロパティにはデフォルトのプロパティが設定され、デフォルトの設定では、電子クレジット決済の際に使用される音は設定されていない。

【０１２９】

また、図９のステップ(904)において、ユーザが電子クレジット決済の安全性よりも操作性を優先する判断をして、バリューパスワードを設定しなかった場合、携帯電話401は、ステップ(905)では、バリューパスワード(VPW)のハッシュ演算は行わず、電子クレジットリスト703の参照データのフィールドには、ヌルが設定してバリューパスワード(VPW)が設定されていないことを示し、ステップ(907)では、バリューパスワード(VPW)のフィールドにヌルを設定して電子クレジット発行要求を送信し、ステップ(909)では、ユーザ識別情報(UID)をハッシュ演算してバリュー認証情報 F(VPW) = Hash(UID)を生成する。

【０１３０】

また、ワレットアプリケーションを終了すると、ユーザが入力したバリューパスワード(VPW)は携帯電話401のメモリから消去される。携帯電話のメモリに保持されている参照データは、バリューパスワードをハッシュ演算したものなので、仮に、携帯電話が第三者に盗まれて、内部のメモリの内容が解析されたとしても、バリューパスワードが知られる心配が無い。

【０１３１】

次に、ダウンロードした電子クレジット(ev)を用いて、電子クレジット決済を行う手順について説明する。図１０は、電子クレジット(ev)を用いた電子クレジット決済の手順を示している。まず、加盟店の店員が電子クレジット決済を開始する操作（決済金額の入力など）を行うと、クレジット決済端末403は、チャレンジ情報として乱数Rを生成する(1000)。この乱数Rはセキュリティカード501から取得したもので、実際にはセキュリティカード501のＣＰＵ516が生成したものである。ユーザがワレットアプリケーションを起動(1001)すると、メニュー画面が表示され(1002)、ユーザがメニュー選択によって使用する電子クレジットを選択して電子クレジット決済操作(1003)を行うと、電子クレジットに対応するバリューパスワードを入力する画面が表示される(1004)。

【０１３２】

ユーザがバリューパスワード(VPW')を入力すると(1005)、携帯電話401は、バリューパスワード(VPW')のハッシュHash(VPW')を計算し、電子クレジットリスト703上の対応する電子クレジットの参照データのHash(VPW)と照合してユーザを認証する(1006)。参照データと一致しなかった場合にはエラーを表示し（図には記載していない）、参照データと一致した場合には、クレジット決済端末403から電子クレジット要求を受信する(1007)。電子クレジット要求には、乱数Rとユーザ端末制御情報が含まれている。ユーザ端末制御情報は、電子クレジット決済時の携帯電話401の動作を制御するための情報であり、クレジットカード会社による設定、及び、加盟店側によって電子クレジット決済を行う環境に応じた制御情報が設定される。具体的には、ユーザ端末制御情報は、ユーザが電子クレジッ

トのプロパティとして設定している効果音の使用の可否や、その音量レベルの制御、さらには、ＬＥＤやバイブレータの動作を制御する情報である。ユーザ端末制御情報によって、例えば、病院などの静かな環境では、大きな音は嫌われるので、その静かな環境でユーザが認識できる程度に音量レベルを低く設定、もしくは、効果音の出力を禁止し、ＬＥＤやバイブレータの動作を制御することで、認証処理が成功したか否かをユーザに明示的に示すことができる。また、繁華街などの騒音が大きい環境では、音量レベルを高く設定して認証処理が成功したか否かをユーザに明示的に示すことが出来る。

【０１３３】

携帯電話401は、ユーザが入力したバリューパスワード(VPW')を用いて、バリュー認証情報 F(VPW')= Hash(VPW'|| UID) 及び 、バリュー認証情報 F(VPW')と乱数Rとの連結のハッシュ Hash(F(VPW') || R)、バリュー認証情報のハッシュ Hash(F(VPW'))をそれぞれ計算し(1008)、クレジット決済端末403に電子クレジットを提示するメッセージとして、電子クレジット(ev)と共にHash(F(VPW') || R)とHash(F(VPW')) とサービス端末制御情報を送信する(1009) 。この時、電子クレジット(ev)の表示用情報805の部分は送信されない。サービス端末制御情報は、電子クレジット決済時のクレジット決済端末403の動作を、制御するための情報であり、ユーザが設定した電子クレジットのプロパティに基づく制御情報が設定される。例えば、具体的には、ユーザ端末制御情報においてユーザが設定した効果音の使用が許可されていて、電子クレジットのプロパティに電子クレジット決済が完了した時に出力される効果音が設定されている場合には、サービス端末制御情報は、クレジット決済端末403の電子クレジット決済が完了した時の音の出力を制限する情報である。

【０１３４】

クレジット決済端末403は、まず、受信した電子クレジット(ev)の電子クレジット公開情報801の内容の有効性を検証（カード番号と有効期限の検証）した後、受信した電子クレジット(ev)とHash(F(VPW') || R)とHash(F(VPW'))を、セキュリティカード501に送り、電子クレジット(ev)とユーザのオフライン認証をセキュリティカード501に行わせる。電子クレジット公開情報801の内容の有効性の検証において、エラーが検出された場合、クレジット決済端末403から携帯電話401にエラーメッセージが送られ、電子クレジット決済の処理を終了する（図には記載していない）。

【０１３５】

セキュリティカード501は、電子クレジット公開情報801の中のカード種別と電子クレジット情報リスト601のカード種別のフィールドとを照合し、以降の処理において、電子クレジット情報リスト601の中のどの種類の電子クレジットに関する情報（マスター鍵(Km)、クレジットカード会社証明書、ネガリスト、アクワイアラ情報、リスク管理情報）を使用するかを特定し、さらに、電子クレジット(ev)のカード番号とネガリストとを照合して、電子クレジット(ev)がネガリストに登録されていないことを検証する(1010)。

【０１３６】

この時、電子クレジット情報リスト601に、受信した電子クレジット(ev)のカード種別が示す種類の電子クレジットが登録されていない場合、または、受信した電子クレジット(ev)がネガリストに登録されていた場合には、セキュリティカード501はクレジット決済端末403に対しエラーを返し、さたに、クレジット決済端末403から携帯電話401にエラーメッセージが送られ、電子クレジット決済の処理を終了する（図には記載していない）。

【０１３７】

次に、セキュリティカード501は、受信したバリュー認証情報のハッシュ Hash(F(VPW'))とマスター鍵Kmの連結のハッシュを計算して電子クレジットのセキュリティ情報800の部分を復号化する共通鍵暗号方式の復号鍵Kc'= Hash(Km || Hash(F(VPW'))))を生成し、コ・プロセッサ520を用いて電子クレジットのセキュリティ情報800を復号化する(1011)。

【０１３８】

さらに、セキュリティカード501は、復号化したセキュリティ情報800からバリュー認証情報803F(VPW)を取り出し、乱数Rとの連結のハッシュ Hash(F(VPW) || R)を計算し、携帯

電話401から受信したHash(F(VPW') || R)と照合し、一致していた場合、ユーザが電子クレジットの正しい所有者であると認証する(1012)。さらに、セキュリティカード501は、コ・プロセッサ520を利用して復号化したセキュリティ情報800の署名情報804が示す電子署名を、クレジットカード会社証明書の中の公開鍵を用いて検証して電子クレジット(ev)が改ざんまたは偽造されていないことを検証する(1013)。Hash(F(VPW) || R)とHash(F(VPW') || R)とが一致しなかった場合、または、署名情報の検証(1013)においてエラーが検出された場合には、セキュリティカード501はクレジット決済端末403に対しエラーを返し、さらに、クレジット決済端末403から携帯電話401にエラーメッセージが送られ、電子クレジット決済の処理を終了する（図には記載していない）。

【０１３９】

署名情報の検証(1013)においてエラーが検出されなかった場合、つまり、電子クレジット(ev)の有効性が検証された場合、セキュリティカード501は、リスク管理情報と電子クレジット(ev)の電子クレジット秘密情報802とから、オンライン認証を行うか否か、決済処理動作を判定する(1014)。

【０１４０】

図１０のステップ(1014)においてオンライン認証を行うと判定した場合、セキュリティカード501はクレジット決済端末403に対してオフライン認証の完了を示すと同時にオンライン認証を要求し、クレジット決済端末403は、携帯電話401に認証結果を送信し(1015)、さらに、アクワイアラ情報に基づいてアクワイアラ404に電子クレジット決済の承認要求を送信し(1017)、さらに、アクワイアラ404がセンター402に電子クレジット決済の承認要求を送信して(1018)、センター402が承認処理を行い(1019)、センター402からアクワイアラ404に承認要求応答が送信され(1020)、さらに、アクワイアラ404からクレジット決済端末403に承認要求応答が送信されて(1021)、クレジット決済端末403での電子クレジット決済処理は完了する。一方、認証結果を受信した携帯電話401は、完了を表示して(1016)、電子クレジット決済処理を完了する。

【０１４１】

また、図１０のステップ(1014)においてオンライン認証を行う必要がないと判定した場合、セキュリティカード501はクレジット決済端末403に対してオフライン認証の完了を示し、クレジット決済端末403は、携帯電話401に認証結果を送信して(1015)、電子クレジット決済処理を完了し、認証結果を受信した携帯電話401は、完了を表示して(1016)、電子クレジット決済処理を完了する。

【０１４２】

また、クレジット決済端末403は、電子クレジット決済処理を完了すると、履歴情報をセキュリティカード501の決済履歴情報602に登録し、電子クレジット情報リスト601に登録されている情報と受信したサービス端末制御情報に基づいて、電子クレジット決済処理が完了したことを示す。例えば、電子クレジット情報リスト601に音声情報が登録されている場合には、クレジット決済端末403はその音声情報を効果音として出力し、また、サービス端末制御情報において音の出力が制限されている場合には、クレジット決済端末403は効果音を出力しない。

【０１４３】

また、携帯電話401は、電子クレジット決済処理を完了すると、その使用した電子クレジットのプロパティと受信したユーザ端末制御情報に基づいて、電子クレジット決済処理が完了したことを示す。例えば、電子クレジットのプロパティに電子クレジット決済が完了した時に出力する音声情報が設定されていて、かつ、ユーザ端末制御情報においてプロパティに設定された効果音の使用が許可され、その音量レベルが指定されている場合、携帯電話401は、指定された音量レベルで、その音声情報を効果音として出力し、また、ユーザ端末制御情報においてプロパティに設定された効果音の使用が禁止されていた場合には、携帯電話401は効果音を出力しない。また、携帯電話401は、クレジット決済端末403からエラーメッセージが送られて電子クレジット決済の処理を終了した場合も、同様にして、その使用した電子クレジットのプロパティと受信したユーザ端末制御情報に基づいて

、電子クレジット決済処理が失敗したことを示す。

【０１４４】

また、電子クレジット決済操作(1003)において、バリューパスワードが設定されていない電子クレジットをユーザが選択した場合には、図１０のステップ(1004)、ステップ(1005)、ステップ(1006)の処理は行わず、携帯電話401はクレジット決済端末403から電子クレジット要求を受信し(1007)、ステップ(1008)の処理では、ユーザ識別情報(UID)をハッシュ演算してバリュー認証情報 F(VPW') = Hash(UID)を計算する。

【０１４５】

また、受信した電子クレジット(ev)の署名情報804が公開鍵暗号方式に基づく電子署名ではなく、電子クレジット公開情報801と、電子クレジット秘密情報802及びバリュー認証情報803とを連結したデータに対するハッシュ演算の結果である種類の電子クレジット(ev)であった場合には、署名情報の検証(1013)の処理では、受信した電子クレジット(ev)の電子クレジット公開情報801と、暗号を復号化した電子クレジット秘密情報802及びバリュー認証情報803とを連結したデータに対するハッシュを計算し、署名情報804と照合して電子クレジット(ev)が改ざんまたは偽造されていないことを検証する。

【０１４６】

また、この電子クレジット決済の場合も、ワレットアプリケーションを終了すると、ユーザが入力したバリューパスワードとバリュー認証情報はメモリから消去される。携帯電話401とクレジット決済端末403との間で交換されるデータの中で、認証処理に用いられるデータは、すべて、ハッシュ演算、または、暗号化されたデータであるため、仮に、第三者によって携帯電話401とクレジット決済端末403との間の通信が盗聴されたとしても、その盗聴したデータを用いて、成りすましを行うことは出来ない。

【０１４７】

次に、ダウンロードした電子クレジット(ev)を用いて、電子クレジット決済を行うもう一つの手順について説明する。図１１は、本実施形態における電子クレジット(ev)を用いた電子クレジット決済のもう一つの手順を示しており、図１０に示した手順では、最初にユーザが自らワレットアプリケーションを起動していたが、図１１に示す手順では、クレジット決済端末403から受信したメッセージに基づいて、ワレットアプリケーションを起動される。

【０１４８】

まず、加盟店の店員が電子クレジット決済を開始する操作（決済金額の入力など）を行うと、クレジット決済端末403は、チャレンジ情報として乱数Rを生成する(1100)。この乱数Rはセキュリティカード501から取得したもので、実際にはセキュリティカード501のＣＰＵ516が生成したものである。ユーザがクレジット決済端末403からのメッセージ受信を可能にする操作を行うと(1101)、携帯電話401はクレジット決済端末403から電子クレジット要求を受信する(1102)。電子クレジット要求には、決済金額と乱数Rとユーザ端末制御情報が含まれている。

【０１４９】

電子クレジット要求を受信した携帯電話401では、ワレットアプリケーションが起動され、受信した決済金額に対してどの電子クレジットを用いるかを問い合わせるダイアログが表示され(1103)、ユーザがメニュー選択によって使用する電子クレジットを選択して電子クレジット決済操作(1104)を行うと、電子クレジットに対応するバリューパスワードを入力する画面が表示される(1105)。

【０１５０】

ユーザがバリューパスワード(VPW')を入力すると(1106)、携帯電話401は、バリューパスワード(VPW')のハッシュHash(VPW')を計算し、電子クレジットリスト703上の対応する電子クレジットの参照データのHash(VPW)と照合してユーザを認証する(1107)。参照データと一致しなかった場合にはエラーを表示し（図には記載していない）、参照データと一致した場合には、携帯電話401は、ユーザが入力したバリューパスワード(VPW')を用いて、バリュー認証情報 F(VPW')= Hash(VPW'|| UID) 及び 、バリュー認証情報 F(VPW')と乱

数Rとの連結のハッシュ Hash(F(VPW') || R)、バリュー認証情報のハッシュ Hash(F(VPW'))をそれぞれ計算し(1108)、クレジット決済端末403に電子クレジットを提示するメッセージとして、電子クレジット(ev)と共にHash(F(VPW') || R)とHash(F(VPW')) とサービス端末制御情報を送信する(1109) 。この時、電子クレジット(ev)の表示用情報805の部分は送信されない。

【０１５１】

クレジット決済端末403は、まず、受信した電子クレジット(ev)の電子クレジット公開情報801の内容の有効性を検証（カード番号と有効期限の検証）した後、受信した電子クレジット(ev)とHash(F(VPW') || R)とHash(F(VPW'))を、セキュリティカード501に送り、電子クレジット(ev)とユーザのオフライン認証をセキュリティカード501に行わせる。電子クレジット公開情報801の内容の有効性の検証において、エラーが検出された場合、クレジット決済端末403から携帯電話401にエラーメッセージが送られ、電子クレジット決済の処理を終了する（図には記載していない）。

【０１５２】

セキュリティカード501は、電子クレジット公開情報801の中のカード種別と電子クレジット情報リスト601のカード種別のフィールドとを照合し、以降の処理において、電子クレジット情報リスト601の中のどの種類の電子クレジットに関する情報（マスター鍵(Km)、クレジットカード会社証明書、ネガリスト、アクワイアラ情報、リスク管理情報）を使用するかを特定し、さらに、電子クレジット(ev)のカード番号とネガリストとを照合して、電子クレジット(ev)がネガリストに登録されていないことを検証する(1110)。

【０１５３】

この時、電子クレジット情報リスト601に、受信した電子クレジット(ev)のカード種別が示す種類の電子クレジットが登録されていない場合、または、受信した電子クレジット(ev)がネガリストに登録されていた場合には、セキュリティカード501はクレジット決済端末403に対しエラーを返し、さたに、クレジット決済端末403から携帯電話401にエラーメッセージが送られ、電子クレジット決済の処理を終了する（図には記載していない）。

【０１５４】

次に、セキュリティカード501は、受信したバリュー認証情報のハッシュ Hash(F(VPW'))とマスター鍵Kmの連結のハッシュを計算して電子クレジットのセキュリティ情報800の部分を復号化する共通鍵暗号方式の復号鍵Kc'= Hash(Km || Hash(F(VPW')))を生成し、コ・プロセッサ520を用いて電子クレジットのセキュリティ情報800を復号化する(1111)。

【０１５５】

さらに、セキュリティカード501は、復号化したセキュリティ情報800からバリュー認証情報803F(VPW)を取り出し、乱数Rとの連結のハッシュ Hash(F(VPW) || R)を計算し、携帯電話401から受信したHash(F(VPW') || R)と照合し、一致していた場合、ユーザが電子クレジットの正しい所有者であると認証する(1112)。さらに、セキュリティカード501は、コ・プロセッサ520を利用して復号化したセキュリティ情報800の署名情報804が示す電子署名を、クレジットカード会社証明書の中の公開鍵を用いて検証して電子クレジット(ev)が改ざんまたは偽造されていないことを検証する(1113)。Hash(F(VPW) || R)とHash(F(VPW') || R)とが一致しなかった場合、または、署名情報の検証(1113)においてエラーが検出された場合には、セキュリティカード501はクレジット決済端末403に対しエラーを返し、さらに、クレジット決済端末403から携帯電話401にエラーメッセージが送られ、電子クレジット決済の処理を終了する（図には記載していない）。

【０１５６】

署名情報の検証(1113)においてエラーが検出されなかった場合、つまり、電子クレジット(ev)の有効性が検証された場合、セキュリティカード501は、リスク管理情報と電子クレジット(ev)の電子クレジット秘密情報802とから、オンライン認証を行うか否か、決済処理動作を判定する(1114)。

【０１５７】

図１１のステップ(1114)においてオンライン認証を行うと判定した場合、セキュリティ

カード501はクレジット決済端末403に対してオフライン認証の完了を示すと同時にオンライン認証を要求し、クレジット決済端末403は、携帯電話401に認証結果を送信し(1115)、さらに、アクワイアラ情報に基づいてアクワイアラ404に電子クレジット決済の承認要求を送信し(1117)、さらに、アクワイアラ404がセンター402に電子クレジット決済の承認要求を送信して(1118)、センター402が承認処理を行い(1119)、センター402からアクワイアラ404に承認要求応答が送信され(1120)、さらに、アクワイアラ404からクレジット決済端末403に承認要求応答が送信されて(1121)、クレジット決済端末403での電子クレジット決済処理は完了する。一方、認証結果を受信した携帯電話401は、完了を表示して(1116)、電子クレジット決済処理を完了する。

【０１５８】

また、図１１のステップ(1114)においてオンライン認証を行う必要がないと判定した場合、セキュリティカード501はクレジット決済端末403に対してオフライン認証の完了を示し、クレジット決済端末403は、携帯電話401に認証結果を送信して(1115)、電子クレジット決済処理を完了し、認証結果を受信した携帯電話401は、完了を表示して(1116)、電子クレジット決済処理を完了する。

【０１５９】

また、クレジット決済端末403は、電子クレジット決済処理を完了すると、履歴情報をセキュリティカード501の決済履歴情報602に登録し、電子クレジット情報リスト601に登録されている情報と受信したサービス端末制御情報に基づいて、電子クレジット決済処理が完了したことを示す。例えば、電子クレジット情報リスト601に音声情報が登録されている場合には、クレジット決済端末403はその音声情報を効果音として出力し、また、サービス端末制御情報において音の出力が制限されている場合には、クレジット決済端末403は効果音を出力しない。

【０１６０】

また、携帯電話401は、電子クレジット決済処理を完了すると、その使用した電子クレジットのプロパティと受信したユーザ端末制御情報に基づいて、電子クレジット決済処理が完了したことを示す。例えば、電子クレジットのプロパティに電子クレジット決済が完了した時に出力する音声情報が設定されていて、かつ、ユーザ端末制御情報においてプロパティに設定された効果音の使用が許可され、その音量レベルが指定されている場合、携帯電話401は、指定された音量レベルで、その音声情報を効果音として出力し、また、ユーザ端末制御情報においてプロパティに設定された効果音の使用が禁止されていた場合には、携帯電話401は効果音を出力しない。また、携帯電話401は、クレジット決済端末403からエラーメッセージが送られて電子クレジット決済の処理を終了した場合も、同様にして、その使用した電子クレジットのプロパティと受信したユーザ端末制御情報に基づいて、電子クレジット決済処理が失敗したことを示す。

【０１６１】

また、電子クレジット決済操作(1104)において、バリューパスワードが設定されていない電子クレジットをユーザが選択した場合には、図１１のステップ(1105)、ステップ(1106)、ステップ(1107)の処理は行わず、携帯電話401はステップ(1108)の処理に進み、ユーザ識別情報(UID)をハッシュ演算してバリュー認証情報 F(VPW') = Hash(UID)を計算する。

【０１６２】

また、受信した電子クレジット(ev)の署名情報804が公開鍵暗号方式に基づく電子署名ではなく、電子クレジット公開情報801と、電子クレジット秘密情報802及びバリュー認証情報803とを連結したデータに対するハッシュ演算の結果である種類の電子クレジット(ev)であった場合には、署名情報の検証(1113)の処理では、受信した電子クレジット(ev)の電子クレジット公開情報801と、暗号を復号化した電子クレジット秘密情報802及びバリュー認証情報803とを連結したデータに対するハッシュを計算し、署名情報804と照合して電子クレジット(ev)が改ざんまたは偽造されていないことを検証する。

【０１６３】

また、この電子クレジット決済の場合も、ワレットアプリケーションを終了すると、ユーザが入力したバリューパスワードとバリュー認証情報はメモリから消去される。携帯電話401とクレジット決済端末403との間で交換されるデータの中で、認証処理に用いられるデータは、すべて、ハッシュ演算、または、暗号化されたデータであるため、仮に、第三者によって携帯電話401とクレジット決済端末403との間の通信が盗聴されたとしても、その盗聴したデータを用いて、成りすましを行うことは出来ない。

【０１６４】

なお、本実施の形態６についての以上の説明では、電子クレジット決済システムについて述べたが、電子クレジットの電子クレジット公開情報801と電子クレジット秘密情報802の部分の内容を変更することで、同様の認証メカニズムを電子デビット決済システムや会員証やＩＤカードなど、他の電子バリューの認証処理にも用いることができる。例えば、電子デビット決済システムの場合には、電子クレジット公開情報801の部分に、銀行口座番号、ユーザ名、発行者名などの情報を入れるだけで良い。

【０１６５】

（実施の形態７）

次に、本発明の第７の実施の形態として、電子チケットシステムについて説明する。本実施の形態７では、電子情報化したチケットである電子チケット（ev：電子バリューの一種）を、複数種類、携帯電話で管理し、ユーザが選択した電子チケット(ev)を用いて、改札装置との間で改札処理が行われる。

【０１６６】

図１２は、電子チケットシステムのブロック構成図を示している。電子チケットシステムは、ユーザが所有する携帯電話1201と、チケット会社のセンター1202と、駅の改札やイベント会場の入口等に設置される改札装置1203と、携帯電話1201とセンター1202間及び改札装置1203とセンター1202間を結ぶネットワーク1204とによって構成される。

【０１６７】

ネットワーク1204は、携帯電話の無線通信ネットワークとインターネットによって構成され、携帯電話1201とセンター1202との無線通信による通信と、改札装置1203とセンター1202とのインターネットによる通信とを可能にする。携帯電話1201とセンター1202との通信及び改札装置1203とセンター1202との通信では、常に、SSL(Secure Sockets Layer)やTLS(Transport Layer Security)などのセキュアセッションを確立され、通信データは暗号化されて伝送される。携帯電話1201と改札装置1203とは、ローカルワイヤレス通信機能（赤外線通信、Bluetooth、無線ＬＡＮ、非接触ＩＣカードの無線通信など）を用いて、アドホックに接続して通信する。

【０１６８】

携帯電話1201には、予め、電子チケット(ev)を管理するワレットアプリケーションがダウンロードされている。また、改札装置1203には、複数種類のチケットの改札処理に対応するため、チケット種別毎にチケット情報が格納され、センター1202と改札装置1203には、電子チケット(ev)の暗号化されている部分を復号化する暗号鍵を生成するためのマスター鍵(Km)か管理されている。

【０１６９】

図１３は、改札装置1203の内部構成を示すブロック図である。改札装置1203は、ゲートのフラップを開閉するゲート機構部1311と、ユーザのゲートへの進入を検出し改札装置1203を起動する起動センサー1312と、ローカルワイヤレス通信Ｉ／Ｆ1313と、ＬＥＤ1314と、スピーカ1315と、それらを制御する制御部1310とによって構成され、制御部1310にはその他の部分を直接制御する制御回路の他に、セキュリティモジュール1300が組み込まれている。

【０１７０】

ローカルワイヤレス通信Ｉ／Ｆ1313は、赤外線通信や、Bluetooth、無線ＬＡＮ、非接触ＩＣカードの無線通信などの通信Ｉ／Ｆであり、携帯電話とアドホックに接続して通信を行うためのものである。

【０１７１】
セキュリテモジュール1300は、マスター鍵(Km)を安全に管理し、電子チケットの認証処理を安全に行うためのデバイスであり、ＴＲＭ部（Tamper Resistant Module）1306と、フラッシュメモリ部1307とによって構成される。ＴＲＭ部1306は、さらに、ＣＰＵ1301と、ＲＯＭ1302と、ＲＡＭ1303と、ＥＥＰＲＯＭ1304と、コ・プロセッサ1305によって構成され、外部からの不正なアクセスを防止する耐タンパ機能を有している。

【０１７２】
フラッシュメモリ部1307には、図１４に示すように、電子チケット情報リスト1401と改札履歴情報1402とが、それぞれ暗号化されて格納されている。電子チケット情報リスト1401は、改札装置が対応する種類の電子チケットに関する情報が登録されたリストであり、改札履歴情報1402は、改札装置が行った電子チケット改札処理の履歴情報である。電子チケット情報リスト1401と改札履歴情報1402の暗号化及び復号化は、ＣＰＵ1301がコ・プロセッサ1305を制御して行う。図１４は、電子チケット情報リスト1401に４種類の電子チケット(ev)に関する情報が登録されている場合を示している。電子チケット情報リスト1401には、１つの種類の電子チケット(ev)に対し、チケット種別、マスター鍵(Km)、チケット会社証明書、ネガリストがそれぞれ登録されている。

【０１７３】
チケット種別は、電子チケット(ev)の種類を示す識別情報であり、マスター鍵(Km)は、この種類の電子チケット(ev)の暗号化されている部分を復号化する暗号鍵を生成するためのマスター鍵、チケット会社証明書は、この種類の電子チケット(ev)を発行しているチケット会社の証明書、ネガリストは、この種類の電子チケット(ev)に関し無効になった電子チケット(ev)のチケット番号（識別情報）のリストである。

【０１７４】
この他、電子チケット情報リスト1401には、電子チケット(ev)の種類ごとに電子チケット改札処理の際に用いる効果音などの音声情報や画像情報などのマルチメディア情報が登録されていても良い。例えば、その電子チケット(ev)の種類またはチケット会社に固有の音声情報や画像情報を登録し、改札処理が完了した際にその効果音をスピーカから出力し、画像情報をＬＣＤに表示することで、その種類（またはチケット会社）の電子チケット(ev)が使用されたことを明示的に示すことができる。

【０１７５】
フラッシュメモリ部1307に格納されている情報へのアクセスは、セキュリティモジュール1300のＣＰＵ1301によって制御されており、改札装置1203は、セキュリティモジュール1300のＴＲＭ部1306を介して、改札履歴情報1402への書込みと読出しを行うことは出来るが、電子チケット情報リスト1401は読出しのみで、書込みを行うことは出来ない。また、電子チケット情報リスト1401の中でも、マスター鍵(Km)は、改札装置1203からは読出しも書込みも出来ないように制御されている。

【０１７６】
電子チケット情報リスト1401は、セキュリティモジュール1300とセンターとが、改札装置1203及びネットワーク1204を介し、暗号化された通信セッションを確立して、必要に応じて更新される。例えば、改札装置1203を管理する事業者とチケット会社との契約に基づき、電子チケット情報の追加や削除が行われ、また、安全性を高めるために、マスター鍵(Km)やネガリストの更新が行われる。

【０１７７】
携帯電話1201は、ローカルワイヤレス通信Ｉ／Ｆを備えており、携帯電話1201のワレットアプリケーションは、ローカルワイヤレス通信Ｉ／Ｆを介して改札装置1203とアドホックに接続し、ワレットアプリケーションが管理している電子チケット(ev)を用いて電子チケット改札処理を行う。また、本実施形態におけるワレットアプリケーションは、第６の実施の形態で説明した電子クレジットを管理し、電子クレジット決済を行う機能も備えている。

【０１７８】

携帯電話1201のメモリ（不揮発性メモリ）には、ワレットアプリケーションが管理する情報として、図１５に示すように、ワレット表示情報1501、ワレット音声情報1502、電子クレジットリスト1503、電子チケットリスト1504が格納されている。ワレット表示情報1501は、ワレットアプリケーションが携帯電話に表示する画面に用いる画像や映像情報などの表示情報であり、ワレット音声情報1502は、ワレットアプリケーションが使用する効果音やメロディ情報などの音声情報、電子チケットリスト1504は、ワレットアプリケーションが管理している電子チケット(ev)のリストである。電子クレジットリスト1503は、第２の実施の形態で説明した電子クレジットリスト703と同様のものであり、ここでは説明を省略する。

【０１７９】

図１５では、電子チケットリスト1504に３つの電子チケット(ev)が登録されている場合を示している。電子チケットリスト1504には、１つの電子チケット(ev)に対し、参照データ、ユーザ識別情報(UID)、電子チケット(ev)、プロパティがそれぞれ登録されている。参照データとユーザ識別情報(UID)については、後で詳しく説明する。

【０１８０】

プロパティは、その電子チケット(ev)に設定された属性情報であり、例えば、ワレットアプリケーションが電子チケットの一覧を表示する際の順番や、電子チケット改札処理の際に使用される効果音や、ＬＥＤやバイブレータなどの動作が設定されている。例えばユーザは、利用頻度に応じて電子チケットが表示される順番を設定したり、電子チケット改札処理が完了した時、または、改札処理が失敗した時に出力される音をワレット音声情報1502からそれぞれ選択して設定したり、電子チケット改札処理が完了した時にＬＥＤを点滅させたり、改札処理が失敗した時にバイブレータを動作させたりといった設定を選択的に行うことができる。

【０１８１】

図１６は、電子チケット(ev)のデータ構造を示している。電子チケットは、大きく分けて、電子チケット公開情報1601とセキュリティ情報1600と表示用情報1605とから構成される。セキュリティ情報1600は、電子チケットの認証処理に用いる情報であり、マスター鍵(Km)から生成される暗号鍵によって暗号化されている。また、表示用情報1605は、ワレットアプリケーションが電子チケットを画面に表示する際に使用する画像やレイアウト情報などの表示情報であり、オプションで設定される。したがって、電子チケット(ev)によって、表示用情報1605を持つものと、持たないものとがある。

【０１８２】

電子チケット公開情報1601は、チケット属性情報、有効期限、発行者名等の電子チケットに関するユーザに公開すべき情報が記述されている部分で、ワレットアプリケーションは、電子チケットを画面に表示する際にこの電子チケット公開情報1601を使用する。チケット属性情報には、電子チケットの種類を示すチケット種別、個々の電子チケットの識別情報であるチケット番号、電子チケットが改札処理済か否かを示す改札済フラグ、電子チケットの使用可能な回数を示す使用可能回数のほか、例えばイベントチケットの場合はイベントの名称や日時、座席番号、会場情報などのそのチケットに関する属性情報が含まれる。

【０１８３】

セキュリティ情報1600は、さらに、電子チケット秘密情報1602と、バリュー認証情報1603と署名情報1604とから構成される。バリュー認証情報1603については、後で詳しく説明する。

【０１８４】

電子チケット秘密情報1602は、チケット会社が設定した顧客管理情報等の電子チケットに関するユーザに必ずしも公開する必要のない情報が記述されている部分で、電子チケット改札処理の際に、改札装置1203側で暗号が復号化され、改札装置1203を管理する事業者またはチケット会社側で必要に応じて使用される情報である。

【０１８５】

署名情報1604は、電子チケット公開情報1601と、暗号化する前の電子チケット秘密情報1602及びバリュー認証情報1603とを連結したデータに対するチケット会社による電子署名であり、電子チケット改札処理の際に、改札装置1203側で暗号が復号化され、電子署名を検証することによって、電子チケット(ev)の有効性の検証に用いられる。

【０１８６】

署名情報1604は、公開鍵暗号方式に基づく、安全性上、充分な鍵長の鍵を用いて生成された電子署名であることが望ましいが、チケット会社の判断で、電子チケット公開情報1601と、暗号化する前の電子チケット秘密情報1602及びバリュー認証情報1603とを連結したデータに対するハッシュ演算の結果であっても良い。

【０１８７】

次に、まず、ユーザがセンター1202から携帯電話1201に電子チケット(ev)をダウンロードする手順について説明する。図１７は、電子チケット(ev)のダウンロードの手順を示している。まず、ユーザが携帯電話1201のインターネットアクセス機能を用いてセンター1202にアクセスして、希望する電子チケットを選択し、また必要に応じて代金の決済処理を行うなど電子チケットを入手する操作を行い(1700)、携帯電話1201とセンター1202との間で入手処理(1701)を行うと、センター1202から携帯電話1201にナビゲーションメッセージ(1702)が送信される。ナビゲーションメッセージ(1702)は、携帯電話1201に電子チケット(ev)のダウンロードを促すメッセージであり、ダウンロードされる電子チケット(ev)を識別するトランザクション番号(TN)が含まれている。

【０１８８】

ナビゲーションメッセージ(1702)を受信した携帯電話1201では、ワレットアプリケーションが起動され、電子チケットをダウンロードするかを問い合わせるダイアログが表示され(1703)、ユーザが電子チケット発行要求操作(1704)を行うと、ダウンロードする電子チケット(ev)に対応してユーザが設定するバリューパスワード(VPW: value password)を入力する画面が表示される(1705)。

【０１８９】

ユーザがバリューパスワードを入力すると(1706)、携帯電話1201は、バリューパスワード(VPW)のハッシュ演算結果 Hash(VPW)をバリューパスワードの参照データとして携帯電話1201のメモリに格納し(1707)、さらに、トランザクション番号(TN)と時刻(T) とから、ユーザ識別情報 UID = Hash(TN || T) (※ ||はデータの連結を示す) を生成してメモリに格納し(1708)、さらに、バリューパスワード(VPW)とユーザ識別情報(UID)とから、バリュー認証情報 F(VPW) = Hash(VPW || UID) を生成し(1709)、トランザクション番号(TN)とバリュー認証情報 F(VPW)を含む電子チケット発行要求をセンター1202に送信する(1710)。この時、参照データHash(VPW)とユーザ識別情報 UID = Hash(TN || T)は、携帯電話1201のメモリ上の電子チケットリスト1504に、新たにダウンロードする電子チケットに関するデータとして、参照データとユーザ識別情報のフィールドにそれぞれ格納される。

【０１９０】

電子チケット発行要求を受信したセンター1202は、トランザクション番号(TN)から発行する電子チケットを特定し(1711)、バリュー認証情報 F(VPW)をハッシュ演算し、マスター鍵Kmと連結して、さらに、ハッシュ演算をして、電子チケット(ev)を暗号化する共通鍵暗号方式の暗号鍵Kt = Hash(Km || Hash(F(VPW)))を生成する(1712)。さらに、センター1202は、電子チケット(ev)の電子チケット公開情報及び電子チケット秘密情報を生成し、受信したバリュー認証情報 F(VPW)と暗号鍵Ktとを用いて、図１６に示したデータ構造を持つ電子チケット(ev)を生成する(1713)。

【０１９１】

生成された電子チケット(ev)は、携帯電話1201に送信され(1714)、電子チケット(ev)は、携帯電話のメモリに格納され(1715)、携帯電話1201がダウンロードの完了を表示して(1716)、電子チケットのダウンロード処理を完了する。この時、電子チケット(ev)は、携帯電話1201のメモリ上の電子チケットリスト1504に、新しい電子チケットとして格納される。また、プロパティにはデフォルトのプロパティが設定され、デフォルトの設定では、電

子チケット改札処理の際に使用される音は設定されていない。

【０１９２】

また、図１７のステップ(1706)において、ユーザが電子チケット改札処理の安全性よりも操作性を優先する判断をして、バリューパスワードを設定しなかった場合、携帯電話1201は、ステップ(1707)では、バリューパスワード(VPW)のハッシュ演算は行わず、電子チケットリスト1504の参照データのフィールドには、ヌルが設定してバリューパスワード(VPW)が設定されていないことを示し、ステップ(1709)では、ユーザ識別情報(UID)をハッシュ演算してバリュー認証情報 F(VPW) = Hash(UID)を生成する。

【０１９３】

また、ワレットアプリケーションを終了すると、ユーザが入力したバリューパスワード(VPW)とバリュー認証情報 F(VPW)は携帯電話1201のメモリから消去される。携帯電話のメモリに保持されている参照データは、バリューパスワードをハッシュ演算したものなので、仮に、携帯電話が第三者に盗まれて、内部のメモリの内容が解析されたとしても、バリューパスワードが知られる心配が無い。

【０１９４】

次に、ダウンロードした電子チケット(ev)を用いて、電子チケット改札処理を行う手順について説明する。図１８は、電子チケット(ev)を用いた電子チケット改札処理の手順を示している。

【０１９５】

まず、ユーザが携帯電話1201を持って改札装置1203のゲートに侵入すると、それを起動センサー1312が検出して改札装置1203を起動し、改札装置1203は、チャレンジ情報として乱数R1を生成する(1800)。この乱数R1はセキュリティモジュール1300から取得したもので、実際にはセキュリティモジュール1300のＣＰＵ1301が生成したものである。ユーザがワレットアプリケーションを起動(1801)すると、メニュー画面が表示され(1802)、ユーザがメニュー選択によって使用する電子チケットを選択して電子チケット使用操作(1803)を行うと、電子チケットに対応するバリューパスワードを入力する画面が表示される(1804)。

【０１９６】

ユーザがバリューパスワード(VPW')を入力すると(1805)、携帯電話1201は、バリューパスワード(VPW')のハッシュHash(VPW')を計算し、電子チケットリスト1504上の対応する電子チケットの参照データのHash(VPW)と照合してユーザを認証する(1806)。参照データと一致しなかった場合にはエラーを表示し（図には記載していない）、参照データと一致した場合には、改札装置1203から電子チケット提示要求を受信する(1807)。電子チケット提示要求には、乱数R1とユーザ端末制御情報が含まれている。ユーザ端末制御情報は、電子チケット改札処理時の携帯電話1201の動作を制御するための情報であり、チケット会社による設定、及び、改札装置を管理する事業者側によって電子チケット改札処理を行う環境に応じた制御情報が設定される。具体的には、ユーザ端末制御情報は、ユーザが電子チケットのプロパティとして設定している効果音の使用の可否や、その音量レベルの制御、さらには、ＬＥＤやバイブレータの動作を制御する情報である。ユーザ端末制御情報によって、例えばクラシックコンサートなどの大きな騒音が嫌われる環境では、ユーザが認識できる程度に音量レベルを低く設定、もしくは、効果音の出力を禁止し、ＬＥＤやバイブレータの動作を制御することで、認証処理が失敗したか否かをユーザに明示的に示すことができる。また、繁華街などの騒音が大きい環境では、音量レベルを大きく設定して認証処理が成功したか否かをユーザに明示的に示すことができる。

【０１９７】

次に、携帯電話1201は、乱数R2を生成し(1808)、さらに、ユーザが入力したバリューパスワード(VPW')を用いて、バリュー認証情報 F(VPW')= Hash(VPW' || UID) 及び 、バリュー認証情報 F(VPW')と乱数R1との連結のハッシュ Hash(F(VPW') || R1)、バリュー認証情報のハッシュ Hash(F(VPW'))をそれぞれ計算し(1809)、改札装置1203に電子チケットを提示するメッセージとして、電子チケット(ev)と共にHash(F(VPW') || R1)とHash(F(VPW')) とサービス端末制御情報を送信する(1810) 。この時、電子チケット(ev)の表示用情

報1605の部分は送信されない。サービス端末制御情報は、電子チケット改札処理時の改札装置1203の動作を、制御するための情報であり、ユーザが設定した電子チケットのプロパティに基づく制御情報が設定される。例えば、具体的には、ユーザ端末制御情報においてユーザが設定した効果音の使用が許可されていて、電子チケットのプロパティに電子チケット改札処理が完了した時に出力される効果音が設定されている場合には、サービス端末制御情報は、改札装置1203の電子チケット改札処理が完了した時の音の出力を制限する情報である。

【０１９８】

改札装置1203は、まず、受信した電子チケット(ev)の電子チケット公開情報1601の内容の有効性を検証（改札済フラグや有効期限、使用可能回数の検証）した後、受信した電子チケット(ev)とHash(F(VPW') || R1)とHash(F(VPW'))を、セキュリティモジュール1300に送り、電子チケット(ev)とユーザのオフライン認証をセキュリティモジュール1300に行わせる。電子チケット公開情報1601の内容の有効性の検証においてエラーが検出された場合、改札装置1203から携帯電話1201にエラーメッセージが送られ、電子チケット改札処理の処理を終了する（図には記載していない）。

【０１９９】

セキュリティモジュール1300は、電子チケット公開情報1601の中のチケット種別と電子チケット情報リスト1401のチケット種別のフィールドとを照合し、以降の処理において、電子チケット情報リスト1401の中のどの種類の電子チケットに関する情報（マスター鍵(Km)、チケット会社証明書）を使用するかを特定し、さらに、電子チケット(ev)のチケット番号とネガリストとを照合して、電子チケット(ev)がネガリストに登録されていないことを検証する(1811)。

【０２００】

この時、電子チケット情報リスト1401に、受信した電子チケット(ev)のチケット種別が示す種類の電子チケットが登録されていない場合、または、受信した電子チケット(ev)がネガリストに登録されていた場合には、セキュリティモジュール1300は改札装置1203に対しエラーを返し、さたに、改札装置1203から携帯電話1201にエラーメッセージが送られ、電子チケット改札処理の処理を終了する（図には記載していない）。

【０２０１】

次に、セキュリティモジュール1300は、受信したバリュー認証情報のハッシュ Hash(F(VPW'))とマスター鍵Kmの連結のハッシュを計算して電子チケットのセキュリティ情報1600の部分を復号化する共通鍵暗号方式の復号鍵Kt'= Hash(Km || Hash(F(VPW')))を生成し、コ・プロセッサ1305を用いて電子チケットのセキュリティ情報1600を復号化する(1812)。

【０２０２】

さらに、セキュリティモジュール1300は、復号化したセキュリティ情報1600からバリュー認証情報1603F(VPW)を取り出し、乱数R1との連結のハッシュ Hash(F(VPW) || R1)を計算し、携帯電話1201から受信したHash(F(VPW') || R1)と照合し、一致していた場合、ユーザが電子チケットの正しい所有者であると認証する(1813)。さらに、セキュリティモジュール1300は、コ・プロセッサ1305を利用して復号化したセキュリティ情報1600の署名情報1604が示す電子署名を、チケット会社証明書の中の公開鍵を用いて検証して電子チケット(ev)が改ざんまたは偽造されていないことを検証する(1814)。Hash(F(VPW) || R1)とHash(F(VPW') || R1)とが一致しなかった場合、または、署名情報の検証(1814)においてエラーが検出された場合には、セキュリティモジュール1300はエラーを返し、改札装置1203から携帯電話1201にエラーメッセージが送られ、電子チケット改札処理の処理を終了する（図には記載していない）。

【０２０３】

署名情報の検証(1814)においてエラーが検出されなかった場合、つまり、電子チケット(ev)の有効性が検証された場合、セキュリティモジュール1300は、電子チケット公開情報1601と電子チケット秘密情報1602の内容を改札処理後の状態に変更し、改札処理した電子チケット(ev')を生成する(1815)。例えばこの時、改札済フラグを立て、使用可能回数を

減算する。この改札処理した電子チケット(ev')の署名情報1604は、電子チケット公開情報1601と、暗号化する前の電子チケット秘密情報1602及びバリュー認証情報1603とを連結したデータに対してハッシュ演算を行った結果である。

【０２０４】

次に、セキュリティモジュール1300は、バリュー認証情報1603F(VPW)と乱数R1と乱数R2との連結のハッシュ Hash(F(VPW) || R1 || R2)を計算して(1816)、電子チケットのオフライン認証の完了を示す。すると、改札装置1203は、携帯電話1201に電子チケットの更新を要求するメッセージとして、電子チケット(ev')と共にHash(F(VPW) || R1 || R2)を送信する(1817)。Hash(F(VPW) || R1 || R2)は、改札装置1203のセキュリティモジュール1300に電子チケット(ev)の電子チケット情報が登録されていて、マスター鍵Kmがなければ生成できない情報であり、携帯電話1201が改札装置1203を認証するため情報となる。

【０２０５】

携帯電話1201は、バリュー認証情報 F(VPW')と乱数R1と乱数R2との連結のハッシュ Hash(F(VPW') || R1 || R2)を計算し、受信したHash(F(VPW) || R1 || R2)と照合し、一致していた場合、改札装置1203がセキュリティモジュール1300に電子チケット(ev)の電子チケット情報が登録された改札装置であると認証し(1818)、電子チケットリスト1504の電子チケット(ev)を受信した改札処理された電子チケット(ev')に更新し(1819)、改札装置1203に対して電子チケットを更新したことを示す更新通知を送信して(1820)、ユーザに完了を表示して(1822)、電子チケット改札処理を完了する。一方、更新通知を受信した改札装置1203は、制御部1306がゲート機構部1307を制御してゲートのフラップを開きユーザの通過を許可して改札装置1203での電子チケット改札処理を完了する(1821)。

【０２０６】

また、改札装置1203は、電子チケット改札処理を完了すると、履歴情報をセキュリティモジュール1300の改札履歴情報1402に登録し、電子チケット情報リスト1401に登録されている情報と受信したサービス端末制御情報に基づいて、電子チケット改札処理が完了したことを示す。例えば、電子チケット情報リスト1401に音声情報が登録されている場合には、改札装置1203はその音声情報を効果音として出力し、また、サービス端末制御情報において音の出力が制限されている場合には、改札装置1203は効果音を出力しない。

【０２０７】

また、携帯電話1201は、電子チケット改札処理を完了すると、その使用した電子チケットのプロパティと受信したユーザ端末制御情報に基づいて、電子チケット改札処理が完了したことを示す。例えば、電子チケットのプロパティに電子チケット改札処理が完了した時に出力する音声情報が設定されていて、かつ、ユーザ端末制御情報においてプロパティに設定された効果音の使用が許可され、その音量レベルが指定されている場合、携帯電話1201は、指定された音量レベルで、その音声情報を効果音として出力し、また、ユーザ端末制御情報においてプロパティに設定された効果音の使用が禁止されていた場合には、携帯電話1201は効果音を出力しない。また、携帯電話1201は、改札装置1203からエラーメッセージが送られて電子チケット改札処理を終了した場合も、同様にして、その使用した電子チケットのプロパティと受信したユーザ端末制御情報に基づいて、電子チケット改札処理が失敗したことを示す。

【０２０８】

また、電子チケット使用操作(1803)において、バリューパスワードが設定されていない電子チケットをユーザが選択した場合には、図１８のステップ（1804）、ステップ（1805）、ステップ（1806）の処理は行わず、携帯電話1201は改札装置1203から電子チケット提示要求を受信し(1807)、ステップ(1809)の処理では、ユーザ識別情報(UID)をハッシュ演算してバリュー認証情報 F(VPW') = Hash(UID)を計算する。

【０２０９】

また、受信した電子チケット(ev)の署名情報1604が公開鍵暗号方式に基づく電子署名ではなく、電子チケット公開情報1601と、電子チケット秘密情報1602及びバリュー認証情報1603とを連結したデータに対するハッシュ演算の結果である種類の電子チケット(ev)であ

った場合には、署名情報の検証(1814)の処理では、受信した電子チケット(ev)の電子チケット公開情報1601と、暗号を復号化した電子チケット秘密情報1602及びバリュー認証情報1603とを連結したデータに対するハッシュを計算し、署名情報1604と照合して電子チケット(ev)が改ざんまたは偽造されていないことを検証する。

【０２１０】

また、この電子チケット改札処理の場合も、ワレットアプリケーションを終了すると、ユーザが入力したバリューパスワードとバリュー認証情報はメモリから消去される。携帯電話1201と改札装置1203との間で交換されるデータの中で、認証処理に用いられるデータは、すべて、ハッシュ演算、または、暗号化されたデータであるため、仮に、第三者によって携帯電話1201と改札装置1203との間の通信が盗聴されたとしても、その盗聴したデータを用いて、成りすましを行うことは出来ない。

【０２１１】

次に、ダウンロードした電子チケット(ev)を用いて、電子チケット改札処理を行うもう一つの手順について説明する。図１９は、本実施形態における電子チケット(ev)を用いた電子チケット改札処理のもう一つの手順を示しており、図１８に示した手順では、最初にユーザが自らワレットアプリケーションを起動していたが、図１９に示す手順では、改札装置1203から受信したメッセージに基づいて、ワレットアプリケーションを起動される。

【０２１２】

まず、ユーザが携帯電話1201を持って改札装置1203のゲートに侵入すると、それを起動センサー1312が検出して改札装置1203を起動し、改札装置1203は、チャレンジ情報として乱数R1を生成する(1900)。この乱数R1はセキュリティモジュール1300から取得したもので、実際にはセキュリティモジュール1300のＣＰＵ1301が生成したものである。ユーザが改札装置1203からのメッセージ受信を可能にする操作を行うと(1901)、携帯電話1201は改札装置1203から電子チケット提示要求を受信する(1902)。電子チケット提示要求には、チケットタイプと乱数R1とユーザ端末制御情報が含まれている。チケットタイプは、電子チケット情報リスト1401に登録されている電子チケットのチケット種別のリストであり、改札装置1203が改札処理できる電子チケットの種類を示す情報である。

【０２１３】

電子チケット提示要求を受信した携帯電話1201では、ワレットアプリケーションが起動され、電子チケットを使用するかをユーザに問い合わせるダイアログが表示される(1903)。この時携帯電話1201は、受信したチケットタイプと電子チケットリスト1504とを照合して改札装置1203で改札処理する電子チケットをユーザに提示する。照合の結果、電子チケットリスト1504に複数該当する電子チケットがあった場合はその一覧を表示し、該当する電子チケットがなかった場合には、該当する電子チケットがないことをユーザに示す（図には記載していない）。

【０２１４】

ユーザが使用する電子チケットを選択して電子チケット使用操作(1904)を行うと、電子チケットに対応するバリューパスワードを入力する画面が表示される(1905)。ユーザがバリューパスワード(VPW')を入力すると(1906)、携帯電話1201は、バリューパスワード(VPW')のハッシュHash(VPW')を計算し、電子チケットリスト1504上の対応する電子チケットの参照データのHash(VPW)と照合してユーザを認証する(1907)。参照データと一致しなかった場合にはエラーを表示し（図には記載していない）、参照データと一致した場合には、携帯電話1201は、乱数R2を生成し(1908)、さらに、ユーザが入力したバリューパスワード(VPW')を用いて、バリュー認証情報 F(VPW')= Hash(VPW'|| UID) 及び 、バリュー認証情報 F(VPW')と乱数R1との連結のハッシュ Hash(F(VPW') || R1)、バリュー認証情報のハッシュ Hash(F(VPW'))をそれぞれ計算し(1909)、改札装置1203に電子チケットを提示するメッセージとして、電子チケット(ev)と共にHash(F(VPW') || R1)とHash(F(VPW')) とサービス端末制御情報を送信する(1910) 。この時、電子チケット(ev)の表示用情報1605の部分は送信されない。

【０２１５】

改札装置1203は、まず、受信した電子チケット(ev)の電子チケット公開情報1601の内容の有効性を検証（改札済フラグや有効期限、使用可能回数の検証）した後、受信した電子チケット(ev)とHash(F(VPW') || R1)とHash(F(VPW'))を、セキュリティモジュール1300に送り、電子チケット(ev)とユーザのオフライン認証をセキュリティモジュール1300に行わせる。電子チケット公開情報1601の内容の有効性の検証においてエラーが検出された場合、改札装置1203から携帯電話1201にエラーメッセージが送られ、電子チケット改札処理の処理を終了する（図には記載していない）。

【０２１６】

セキュリティモジュール1300は、電子チケット公開情報1601の中のチケット種別と電子チケット情報リスト1401のチケット種別のフィールドとを照合し、以降の処理において、電子チケット情報リスト1401の中のどの種類の電子チケットに関する情報（マスター鍵(Km)、チケット会社証明書）を使用するかを特定し、さらに、電子チケット(ev)のチケット番号とネガリストとを照合して、電子チケット(ev)がネガリストに登録されていないことを検証する(1911)。

【０２１７】

この時、電子チケット情報リスト1401に、受信した電子チケット(ev)のチケット種別が示す種類の電子チケットが登録されていない場合、または、受信した電子チケット(ev)がネガリストに登録されていた場合には、セキュリティモジュール1300は改札装置1203に対しエラーを返し、さたに、改札装置1203から携帯電話1201にエラーメッセージが送られ、電子チケット改札処理の処理を終了する（図には記載していない）。

【０２１８】

次に、セキュリティモジュール1300は、受信したバリュー認証情報のハッシュ Hash(F(VPW'))とマスター鍵Kmの連結のハッシュを計算して電子チケットのセキュリティ情報1600の部分を復号化する共通鍵暗号方式の復号鍵Kt'= Hash(Km || Hash(F(VPW')))を生成し、コ・プロセッサ1305を用いて電子チケットのセキュリティ情報1600を復号化する(1912)。

【０２１９】

さらに、セキュリティモジュール1300は、復号化したセキュリティ情報1600からバリュー認証情報1603F(VPW)を取り出し、乱数R1との連結のハッシュ Hash(F(VPW) || R1)を計算し、携帯電話1201から受信したHash(F(VPW') || R1)と照合し、一致していた場合、ユーザが電子チケットの正しい所有者であると認証する(1913)。さらに、セキュリティモジュール1300は、コ・プロセッサ1305を利用して復号化したセキュリティ情報1600の署名情報1604が示す電子署名を、チケット会社証明書の中の公開鍵を用いて検証して電子チケット(ev)が改ざんまたは偽造されていないことを検証する(1914)。Hash(F(VPW) || R1)とHash(F(VPW') || R1)とが一致しなかった場合、または、署名情報の検証(1914)においてエラーが検出された場合には、セキュリティモジュール1300はエラーを返し、改札装置1203から携帯電話1201にエラーメッセージが送られ、電子チケット改札処理の処理を終了する（図には記載していない）。

【０２２０】

署名情報の検証(1914)においてエラーが検出されなかった場合、つまり、電子チケット(ev)の有効性が検証された場合、セキュリティモジュール1300は、電子チケット公開情報1601と電子チケット秘密情報1602の内容を改札処理後の状態に変更し、改札処理した電子チケット(ev')を生成する(1915)。例えばこの時、改札済フラグを立て、使用可能回数を減算する。この改札処理した電子チケット(ev')の署名情報1604は、電子チケット公開情報1601と、暗号化する前の電子チケット秘密情報1602及びバリュー認証情報1603とを連結したデータに対してハッシュ演算を行った結果である。

【０２２１】

次に、セキュリティモジュール1300は、バリュー認証情報1603F(VPW)と乱数R1と乱数R2との連結のハッシュ Hash(F(VPW) || R1 || R2)を計算して(1916)、電子チケットのオフライン認証の完了を示す。すると、改札装置1203は、携帯電話1201に電子チケットの更新を要求するメッセージとして、電子チケット(ev')と共にHash(F(VPW) || R1 || R2)を送

信する(1917)。Hash(F(VPW) || R1 || R2)は、改札装置1203のセキュリティモジュール1300に電子チケット(ev)の電子チケット情報が登録されていて、マスター鍵Kmがなければ生成できない情報であり、携帯電話1201が改札装置1203を認証するため情報となる。

【０２２２】

携帯電話1201は、バリュー認証情報 F(VPW')と乱数R1と乱数R2との連結のハッシュ Hash(F(VPW') || R1 || R2)を計算し、受信したHash(F(VPW) || R1 || R2)と照合し、一致していた場合、改札装置1203がセキュリティモジュール1300に電子チケット(ev)の電子チケット情報が登録された改札装置であると認証し(1918)、電子チケットリスト1504の電子チケット(ev)を受信した改札処理された電子チケット(ev')に更新し(1919)、改札装置1203に対して電子チケットを更新したことを示す更新通知を送信して(1920)、ユーザに完了を表示して(1922)、電子チケット改札処理を完了する。一方、更新通知を受信した改札装置1203は、制御部1306がゲート機構部1307を制御してゲートのフラップを開きユーザの通過を許可して改札装置1203での電子チケット改札処理を完了する(1921)。

【０２２３】

また、改札装置1203は、電子チケット改札処理を完了すると、履歴情報をセキュリティモジュール1300の改札履歴情報1402に登録し、電子チケット情報リスト1401に登録されている情報と受信したサービス端末制御情報に基づいて、電子チケット改札処理が完了したことを示す。例えば、電子チケット情報リスト1401に音声情報が登録されている場合には、改札装置1203はその音声情報を効果音として出力し、また、サービス端末制御情報において音の出力が制限されている場合には、改札装置1203は効果音を出力しない。

【０２２４】

また、携帯電話1201は、電子チケット改札処理を完了すると、その使用した電子チケットのプロパティと受信したユーザ端末制御情報に基づいて、電子チケット改札処理が完了したことを示す。例えば、電子チケットのプロパティに電子チケット改札処理が完了した時に出力する音声情報が設定されていて、かつ、ユーザ端末制御情報においてプロパティに設定された効果音の使用が許可され、その音量レベルが指定されている場合、携帯電話1201は、指定された音量レベルで、その音声情報を効果音として出力し、また、ユーザ端末制御情報においてプロパティに設定された効果音の使用が禁止されていた場合には、携帯電話1201は効果音を出力しない。また、携帯電話1201は、改札装置1203からエラーメッセージが送られて電子チケット改札処理を終了した場合も、同様にして、その使用した電子チケットのプロパティと受信したユーザ端末制御情報に基づいて、電子チケット改札処理が失敗したことを示す。

【０２２５】

また、電子チケット使用操作(1903)において、バリューパスワードが設定されていない電子チケットをユーザが選択した場合には、図１９のステップ（1905）、ステップ（1906）、ステップ（1907）の処理は行わず、携帯電話1201はステップ(1908)の処理に進み、さらに、ステップ(1909)の処理では、ユーザ識別情報(UID)をハッシュ演算してバリュー認証情報 F(VPW') = Hash(UID)を計算する。

【０２２６】

また、受信した電子チケット(ev)の署名情報1604が公開鍵暗号方式に基づく電子署名ではなく、電子チケット公開情報1601と、電子チケット秘密情報1602及びバリュー認証情報1603とを連結したデータに対するハッシュ演算の結果である種類の電子チケット(ev)であった場合には、署名情報の検証(1914)の処理では、受信した電子チケット(ev)の電子チケット公開情報1601と、暗号を復号化した電子チケット秘密情報1602及びバリュー認証情報1603とを連結したデータに対するハッシュを計算し、署名情報1604と照合して電子チケット(ev)が改ざんまたは偽造されていないことを検証する。

【０２２７】

また、この電子チケット改札処理の場合も、ワレットアプリケーションを終了すると、ユーザが入力したバリューパスワードとバリュー認証情報はメモリから消去される。携帯電話1201と改札装置1203との間で交換されるデータの中で、認証処理に用いられるデータ

は、すべて、ハッシュ演算、または、暗号化されたデータであるため、仮に、第三者によって携帯電話1201と改札装置1203との間の通信が盗聴されたとしても、その盗聴したデータを用いて、成りすましを行うことは出来ない。

【０２２８】

なお、本実施の形態７についての以上の説明では、電子チケットシステムについて述べたが、電子チケットの電子チケット公開情報1601と電子チケット秘密情報1602の部分の内容を変更することで、同様の認証メカニズムを電子クーポンシステムや電子マネーシステムなど、他の電子バリューの認証処理にも用いることができる。例えば、電子クーポンシステムの場合には、電子チケット公開情報1601の部分に、割引率などのクーポンによって提供されるサービスに関する情報を入れるだけで良く、また、電子マネーシステムの場合には、電子チケット公開情報1601の部分に、使用可能回数の代わりに電子マネーの残金を示す情報を入れ、改札処理時に改札装置が利用金額を減算するようにすれば良い。

【０２２９】

（実施の形態８）

次に、本発明の第８の実施形態として、業務用途向けの電子鍵システムについて説明する。本実施の形態８では、電子情報化した鍵である電子鍵（ev：電子バリューの一種）を、複数種類、携帯電話で管理し、ユーザが選択した電子鍵(ev)を用いて、錠前装置との間で認証処理が行われる。

【０２３０】

図２０は、電子鍵システムのブロック構成図を示している。電子鍵システムは、ユーザが所有する携帯電話2001と、会議室や集会場などの施設やレンタカーなどの設備を管理している管理会社のセンター2002と、会議室や自動車のドアなどに取り付けられる錠前装置2003と、携帯電話2001とセンター2002を結ぶネットワーク2004とによって構成される。本実施形態の電子鍵システムによれば、ユーザは鍵を電子鍵(ev)としてセンター2002から携帯電話2001にダウンロードして、錠前装置2003を開錠または施錠することができ、物理的な鍵の受け渡しが発生しないため、ユーザは鍵を管理している所に鍵を取りに行く必要がなく、また、管理する側も鍵の受け渡しを行う担当者を置く必要がなく、業務の効率化を図ることができる。

【０２３１】

ネットワーク2004は、携帯電話の無線通信ネットワークとインターネットによって構成され、携帯電話2001とセンター2002との無線通信による通信を可能にする。携帯電話2001とセンター2002との通信では、常に、SSL(Secure Sockets Layer)やTLS(Transport Layer Security)などのセキュアセッションを確立され、通信データは暗号化されて伝送される。

【０２３２】

携帯電話2001と錠前装置2003とは、ローカルワイヤレス通信機能（赤外線通信、Bluetooth、無線ＬＡＮ、非接触ＩＣカードの無線通信など）を用いて、アドホックに接続して通信する。携帯電話2001には、予め、電子鍵(ev)を管理するワレットアプリケーションがダウンロードされている。また、センター2002と錠前装置2003には、電子鍵(ev)の暗号化されている部分を復号化する暗号鍵を生成するためのマスター鍵(Km)か管理されている。安全上、マスター鍵(Km)は、錠前装置2003ごとに異なっていることが望ましいが、適当な数の錠前装置2003の単位で、同じマスター鍵(Km)を用いても良い。センター2002では錠前装置2003ごとに、どのマスター鍵(Km)を使用しているかを管理している。

【０２３３】

図２１は、錠前装置2003の内部構成を示すブロック図である。錠前装置2003は、物理的にロックの開閉を錠前機構部2111と、ユーザの操作を検出して錠前装置2003を起動する起動センサー2112と、ローカルワイヤレス通信Ｉ／Ｆ2113と、錠前装置2003の状態を示すＬＥＤ2114と、制御スイッチ2115と、それらを制御する制御部2110とによって構成され、制御部2110にはその他の部分を直接制御する制御回路の他に、セキュリティモジュール2100が組み込まれている。ローカルワイヤレス通信Ｉ／Ｆ2113は、赤外線通信や、Bluetooth

、無線ＬＡＮ、非接触ＩＣカードの無線通信などの通信Ｉ／Ｆであり、携帯電話とアドホックに接続して通信を行うためのものである。

【０２３４】

セキュリティモジュール2100は、マスター鍵(Km)を安全に管理し、電子鍵の認証処理を安全に行うためのデバイスであり、セキュリティモジュール2100は、ＣＰＵ2101と、ＲＯＭ2102と、ＲＡＭ2103と、ＥＥＰＲＯＭ2104と、コ・プロセッサ2105によって構成され、外部からの不正なアクセスを防止する耐タンパ機能を有している。

【０２３５】

ＥＥＰＲＯＭ2104には、錠前ＩＤ、マスター鍵(Km)、管理会社公開鍵が格納されている。錠前ＩＤは、錠前装置2003の識別情報であり、マスター鍵(Km)は、この錠前装置2003の電子鍵(ev)の暗号化されている部分を復号化する暗号鍵を生成するためのマスター鍵、管理会社公開鍵は、この錠前装置2003の電子鍵(ev)を発行する管理会社の公開鍵である。

【０２３６】

セキュリティモジュール2100のＥＥＰＲＯＭ2104に格納されている情報へのアクセスは、ＣＰＵ2101によって制御されており、制御部2110のその他の制御回路から、錠前ＩＤと管理会社公開鍵は読み出すことはできるが、書き換えはできない。また、マスター鍵(Km)は、読出しも書込みも出来ないように制御されている。

【０２３７】

携帯電話2001は、ローカルワイヤレス通信Ｉ／Ｆを備えており、携帯電話2001のワレットアプリケーションは、ローカルワイヤレス通信Ｉ／Ｆを介して錠前装置2003とアドホックに接続し、ワレットアプリケーションが管理している電子鍵(ev)を用いて電子鍵の認証処理を行う。また、本実施の形態８におけるワレットアプリケーションは、第２の実施の形態で説明した電子クレジットと第３の実施の形態で説明した電子チケットを管理し、電子クレジット決済や電子チケット改札処理を行う機能も備えている。

【０２３８】

携帯電話2001のメモリ（不揮発性メモリ）には、ワレットアプリケーションが管理する情報として、図２２に示すように、ワレット表示情報2201、ワレット音声情報2202、電子クレジットリスト2203、電子チケットリスト2204、電子鍵リスト2205が格納されている。ワレット表示情報2201は、ワレットアプリケーションが携帯電話に表示する画面に用いる画像や映像情報などの表示情報であり、ワレット音声情報2202は、ワレットアプリケーションが使用する効果音やメロディ情報などの音声情報、電子鍵リスト2205は、ワレットアプリケーションが管理している電子鍵(ev)のリストである。電子クレジットリスト2203は、第２の実施の形態で説明した電子クレジットリスト703と同様のものであり、また、電子チケットリスト2204は、第３の実施の形態で説明した電子チケットリスト1504と同様のものであり、ここでは説明を省略する。

【０２３９】

図２２では、電子鍵リスト2205に３つの電子鍵(ev)が登録されている場合を示している。電子鍵リスト2205には、１つの電子鍵(ev)に対し、参照データ、ユーザ識別情報(UID)、電子鍵(ev)、プロパティがそれぞれ登録されている。参照データとユーザ識別情報(UID)については、後で詳しく説明する。

【０２４０】

プロパティは、その電子鍵(ev)に設定された属性情報であり、例えば、ワレットアプリケーションが電子鍵の一覧を表示する際の順番や、電子鍵の認証処理の際に使用される効果音や、ＬＥＤやバイブレータなどの動作が設定されている。例えばユーザは、利用頻度に応じて電子鍵が表示される順番を設定したり、電子鍵の認証処理が完了した時、または、認証処理が失敗した時に出力される音をワレット音声情報2202からそれぞれ選択して設定したり、電子鍵の認証処理が完了した時にＬＥＤを点滅させたり、認証処理が失敗した時にバイブレータを動作させたりといった設定を選択的に行うことができる。

【０２４１】

図２３は、電子鍵(ev)のデータ構造を示している。電子鍵は、大きく分けて、電子鍵公

開情報2301とセキュリティ情報2300と表示用情報2305とから構成される。セキュリティ情報2300は、電子鍵の認証処理に用いる情報であり、マスター鍵(Km)から生成される暗号鍵によって暗号化されている。また、表示用情報2305は、ワレットアプリケーションが電子鍵を画面に表示する際に使用する画像情報などの表示情報であり、オプションで設定される。したがって、電子鍵(ev)によって、表示用情報2305を持つものと、持たないものとがある。例えば、会議室の電子鍵の場合には、会議室の場所を示す地図や見取図どの情報が表示用情報として設定される。

【０２４２】

電子鍵公開情報2301は、鍵の名称、鍵ＩＤ、錠前ＩＤ、有効期限、発行者名等の電子鍵に関するユーザに公開すべき情報が記述されている部分で、ワレットアプリケーションは、電子鍵を画面に表示する際にこの電子鍵公開情報2301を使用する。

【０２４３】

セキュリティ情報2300は、さらに、電子鍵秘密情報2302と、バリュー認証情報2303と署名情報2304とから構成される。バリュー認証情報2303については、後で詳しく説明する。

【０２４４】

電子鍵秘密情報2302は、錠前装置2003を管理する管理会社が設定した顧客管理情報等の電子鍵に関するユーザに必ずしも公開する必要のない情報が記述されている部分で、電子鍵の認証処理の際に、錠前装置2003側で暗号が復号化され、管理会社側で必要に応じて使用される情報である。

【０２４５】

署名情報2304は、電子鍵公開情報2301と、暗号化する前の電子鍵秘密情報2302及びバリュー認証情報2303とを連結したデータに対する管理会社による電子署名であり、電子鍵の認証処理の際に、錠前装置2003側で暗号が復号化され、電子署名を検証することによって、電子鍵(ev)の有効性の検証に用いられる。

【０２４６】

署名情報2304は、公開鍵暗号方式に基づく、安全性上、充分な鍵長の鍵を用いて生成された電子署名であることが望ましいが、管理会社の判断で、電子鍵公開情報2301と、暗号化する前の電子鍵秘密情報2302及びバリュー認証情報2303とを連結したデータに対するハッシュ演算の結果であっても良い。

【０２４７】

次に、まず、ユーザがセンター2002から携帯電話2001に電子鍵(ev)をダウンロードする手順について説明する。図２４は、電子鍵(ev)のダウンロードの手順を示している。まず、ユーザが携帯電話2001のインターネットアクセス機能を用いてセンター2002にアクセスして、会議室などの施設やレンタカーなどを予約し、また必要に応じて代金の決済処理を行うなど電子鍵を入手する操作を行い(2400)、携帯電話2001とセンター2002との間で入手処理(2401)を行うと、センター2002から携帯電話2001にナビゲーションメッセージ(2402)が送信される。ナビゲーションメッセージ(2402)は、携帯電話2001に電子鍵(ev)のダウンロードを促すメッセージであり、ダウンロードされる電子鍵(ev)を識別するトランザクション番号(TN)が含まれている。

【０２４８】

ナビゲーションメッセージ(2402)を受信した携帯電話2001では、ワレットアプリケーションが起動され、電子鍵をダウンロードするかを問い合わせるダイアログが表示され(2403)、ユーザが電子鍵発行要求操作(2404)を行うと、ダウンロードする電子鍵(ev)に対応してユーザが設定するバリューパスワード(VPW: value password)を入力する画面が表示される(2405)。

【０２４９】

ユーザがバリューパスワードを入力すると(2406)、携帯電話2001は、バリューパスワード(VPW)のハッシュ演算結果 Hash(VPW)をバリューパスワードの参照データとして携帯電話2001のメモリに格納し(2407)、さらに、トランザクション番号(TN)と時刻(T) とから、ユーザ識別情報 UID = Hash(TN || T) （※ ||はデータの連結を示す） を生成してメモリ

に格納し(2408)、さらに、バリューパスワード(VPW)とユーザ識別情報(UID)とから、バリュー認証情報 F(VPW) = Hash(VPW || UID) を生成し(2409)、トランザクション番号(TN)とバリュー認証情報 F(VPW)を含む電子鍵発行要求をセンター2002に送信する(2410) 。この時、参照データHash(VPW)とユーザ識別情報 UID = Hash(TN || T)は、携帯電話2001のメモリ上の電子鍵リスト2204に、新たにダウンロードする電子鍵に関するデータとして、参照データとユーザ識別情報のフィールドにそれぞれ格納される。

【０２５０】

電子鍵発行要求を受信したセンター2002は、トランザクション番号(TN)から発行する電子鍵を特定し(2411)、バリュー認証情報 F(VPW)をハッシュ演算し、マスター鍵Kmと連結して、さらに、ハッシュ演算をして、電子鍵(ev)を暗号化する共通鍵暗号方式の暗号鍵Kk = Hash(Km || Hash(F(VPW)))を生成する(2412)。さらに、センター2002は、電子鍵(ev)の電子鍵公開情報及び電子鍵秘密情報を生成し、受信したバリュー認証情報 F(VPW)と暗号鍵Kkとを用いて、図２３に示したデータ構造を持つ電子鍵(ev)を生成する(2413)。この時、電子鍵(ev)の有効期限には、ステップ(2401)の入手処理における予約内容に基づく有効期限が設定される。例えば、会議室の電子鍵(ev)の場合には、電子鍵(ev)の有効期限には、会議室を予約した時間帯に基づく有効期限が設定される。

【０２５１】

生成された電子鍵(ev)は、携帯電話2001に送信され(2414)、電子鍵(ev)は、携帯電話のメモリに格納され(2415)、携帯電話2001がダウンロードの完了を表示して(2416)、電子鍵のダウンロード処理を完了する。この時、電子鍵(ev)は、携帯電話2001のメモリ上の電子鍵リスト2204に、新しい電子鍵として格納される。また、プロパティにはデフォルトのプロパティが設定され、デフォルトの設定では、電子鍵の認証処理の際に使用される音は設定されていない。

【０２５２】

また、図２４のステップ(2406)において、ユーザが電子鍵の認証処理の安全性よりも操作性を優先する判断をして、バリューパスワードを設定しなかった場合、携帯電話2001は、ステップ(2407)では、バリューパスワード(VPW)のハッシュ演算は行わず、電子鍵リスト2204の参照データのフィールドには、ヌルが設定してバリューパスワード(VPW)が設定されていないことを示し、ステップ(2409)では、ユーザ識別情報(UID)をハッシュ演算してバリュー認証情報 F(VPW) = Hash(UID)を生成する。

【０２５３】

また、ワレットアプリケーションを終了すると、ユーザが入力したバリューパスワード(VPW)とバリュー認証情報 F(VPW)は携帯電話2001のメモリから消去される。携帯電話のメモリに保持されている参照データは、バリューパスワードをハッシュ演算したものなので、仮に、携帯電話が第三者に盗まれて、内部のメモリの内容が解析されたとしても、バリューパスワードが知られる心配が無い。

【０２５４】

次に、ダウンロードした電子鍵(ev)を用いて、錠前装置2003との間で認証処理を行い、錠前装置2003を開錠（または施錠）する手順について説明する。図２５は、本実施形態における電子鍵(ev)を用いた認証処理の手順を示している。

【０２５５】

まず、ユーザが、錠前装置2003が取り付けられている扉のハンドルに手をかけるなど、錠前装置2003を起動にさせる操作(2500)を行うと、錠前装置2003の起動センサー2112がそれを検出して錠前装置2003を起動し、錠前装置2003は、チャレンジ情報として乱数Rを生成する(2501)。この乱数Rはセキュリティモジュール2100から取得したもので、実際にはセキュリティモジュール2100のＣＰＵ2101が生成したものである。ユーザが錠前装置2003からのメッセージ受信を可能にする操作を行うと(2502)、携帯電話2001は錠前装置2003から電子鍵提示要求を受信する(2503)。電子鍵提示要求には、錠前ＩＤと乱数Rが含まれている。

【０２５６】

電子鍵提示要求を受信した携帯電話2001では、ワレットアプリケーションが起動され、電子鍵を使用するかをユーザに問い合わせるダイアログが表示される(2504)。この時、携帯電話2001は、受信した錠前ＩＤと電子鍵リスト2205とを照合して、その錠前装置2003の電子鍵をユーザに提示する。該当する電子鍵がなかった場合には、該当する電子鍵がないことをユーザに示す（図には記載していない）。

【０２５７】

ユーザが電子鍵使用操作(2505)を行うと、電子鍵に対応するバリューパスワードを入力する画面が表示される(2506)。ユーザがバリューパスワード(VPW')を入力すると(2507)、携帯電話2001は、バリューパスワード(VPW')のハッシュHash(VPW')を計算し、電子鍵リスト2204上の対応する電子鍵の参照データのHash(VPW)と照合してユーザを認証する(2508)。参照データと一致しなかった場合にはエラーを表示し（図には記載していない）、参照データと一致した場合には、携帯電話2001は、ユーザが入力したバリューパスワード(VPW')を用いて、バリュー認証情報 F(VPW')= Hash(VPW' || UID) 及び 、バリュー認証情報 F(VPW')と乱数Rとの連結のハッシュ Hash(F(VPW') || R)、バリュー認証情報のハッシュ Hash(F(VPW'))をそれぞれ計算し(2509)、錠前装置2003に電子鍵を提示するメッセージとして、電子鍵(ev)と共にHash(F(VPW') || R)とHash(F(VPW'))を送信する(2510)。この時、電子鍵(ev)の表示用情報2305の部分は送信されない。

【０２５８】

錠前装置2003は、まず、受信した電子鍵(ev)の電子鍵公開情報2301の内容の有効性を検証（錠前ＩＤと有効期限の検証）した後、受信した電子鍵(ev)とHash(F(VPW') || R)とHash(F(VPW'))を、セキュリティモジュール2100に送り、電子鍵(ev)とユーザのオフライン認証をセキュリティモジュール2100に行わせる。電子鍵公開情報2301の内容の有効性の検証（錠前ＩＤと有効期限の検証）においてエラーが検出された場合、錠前装置2003から携帯電話2001にエラーメッセージが送られ、電子鍵の認証処理を終了する（図には記載していない）。つまり、有効期限が過ぎた電子鍵(ev)は自動的に使用できなくなるので、使用後、電子鍵を返却する必要はない。

【０２５９】

セキュリティモジュール2100は、受信したバリュー認証情報のハッシュ Hash(F(VPW'))とマスター鍵Kmの連結のハッシュを計算して電子鍵のセキュリティ情報2300の部分を復号化する共通鍵暗号方式の復号鍵Kk'= Hash(Km || Hash(F(VPW')))を生成し、コ・プロセッサ2105を用いて電子鍵のセキュリティ情報2300を復号化する(2511)。

【０２６０】

さらに、セキュリティモジュール2100は、復号化したセキュリティ情報2300からバリュー認証情報2303F(VPW)を取り出し、乱数Rとの連結のハッシュ Hash(F(VPW) || R)を計算し、携帯電話2001から受信したHash(F(VPW') || R)と照合し、一致していた場合、ユーザが電子鍵の正しい所有者であると認証する(2512)。さらに、セキュリティモジュール2100は、コ・プロセッサ2105を利用して復号化したセキュリティ情報2300の署名情報2304が示す電子署名を、管理会社公開鍵を用いて検証して電子鍵(ev)が改ざんまたは偽造されていないことを検証する(2513)。Hash(F(VPW) || R)とHash(F(VPW') || R)とが一致しなかった場合、または、署名情報の検証(2513)においてエラーが検出された場合には、セキュリティモジュール2100は錠前装置2003に対しエラーを返し、さらに、錠前装置2003から携帯電話2001にエラーメッセージが送られ、電子鍵の認証処理を終了する（図には記載していない）。

【０２６１】

署名情報の検証(2513)においてエラーが検出されなかった場合、つまり、電子鍵(ev)の有効性が検証された場合、セキュリティモジュール2100は錠前装置2003に対してオフライン認証の完了を示し、錠前装置2003は、携帯電話2001に認証結果を送信して(2514)、認証処理を完了し、認証結果を受信した携帯電話2001は、完了を表示して(2516)、電子鍵の認証処理を完了する。

【０２６２】

また、錠前装置2003は、制御部2106が錠前機構部2107を制御して錠前装置2103のロックを開錠（または施錠）し、錠前装置2003での電子鍵の認証処理を完了する(2515)。

【０２６３】

また、携帯電話2001は、電子鍵の認証処理を完了すると、その使用した電子鍵のプロパティに基づいて、認証処理が完了したことを示す。また、携帯電話2001は、錠前装置2003からエラーメッセージが送られて電子鍵の認証処理を終了した場合も、同様にして、その使用した電子鍵のプロパティに基づいて、電子鍵の認証処理が失敗したことを示す。

【０２６４】

また、電子鍵使用操作(2505)において、バリューパスワードが設定されていない電子鍵をユーザが選択された場合には、図２５のステップ(2506)、ステップ(2507)、ステップ(2508)の処理は行わず、携帯電話2001はステップ(2509)の処理に進み、ユーザ識別情報(UID)をハッシュ演算してバリュー認証情報 F(VPW') = Hash(UID)を計算する。

【０２６５】

また、受信した電子鍵(ev)の署名情報2304が公開鍵暗号方式に基づく電子署名ではなく、電子鍵公開情報2301と、電子鍵秘密情報2302及びバリュー認証情報2303とを連結したデータに対するハッシュ演算の結果である種類の電子鍵(ev)であった場合には、署名情報の検証(2513)の処理では、受信した電子鍵(ev)の電子鍵公開情報2301と、暗号を復号化した電子鍵秘密情報2302及びバリュー認証情報2303とを連結したデータに対するハッシュを計算し、署名情報2304と照合して電子鍵(ev)が改ざんまたは偽造されていないことを検証する。

【０２６６】

また、この電子鍵の認証処理の場合も、ワレットアプリケーションを終了すると、ユーザが入力したバリューパスワードとバリュー認証情報はメモリから消去される。携帯電話2001と錠前装置2003との間で交換されるデータの中で、認証処理に用いられるデータは、すべて、ハッシュ演算、または、暗号化されたデータであるため、仮に、第三者によって携帯電話2001と錠前装置2003との間の通信が盗聴されたとしても、その盗聴したデータを用いて、成りすましを行うことは出来ない。

【０２６７】

（実施の形態９）

次に、本発明の第９の実施の形態として、家庭用途向けの電子鍵システムについて説明する。本実施の形態９では、電子情報化した鍵である電子鍵（ev：電子バリューの一種）を錠前装置が携帯電話に発行し、その電子鍵(ev)を用いて、携帯電話と錠前装置との間で認証処理を行うことによって、錠前の開錠または施錠を行う。

【０２６８】

本電子鍵システムのブロック構成は、基本的に第４の実施の形態の場合と同じであり、図２０が本電子鍵システムのブロック構成を示している。電子鍵システムは、ユーザが所有する携帯電話2001と、センター2002と、錠前装置2003と、携帯電話2001とセンター2002を結ぶネットワーク2004とによって構成される。但し、錠前装置2003は、家庭用のもので、家のドアに取り付けられたり、ユーザが購入して取り付けを行ったりすることができる形態のものである。また、センター2002は、錠前装置2003を製造または販売する事業者、または、携帯電話2001にダウンロードするワレットアプリケーションを提供する事業者によって運営されるセンター装置である。本電子鍵システムにおいて、センター2002は、携帯電話2001に電子鍵(ev)を管理するワレットアプリケーションをダウンロードするためのものであり、予め、携帯電話2001にワレットアプリケーションが搭載、または、ダウンロードされている場合にはセンター2002は必要ない。

【０２６９】

本実施の形態９の電子鍵システムによれば、ユーザの管理のもとに、複数の携帯電話2001に対して錠前装置2003の電子鍵(ev)を発行することができ、また、その無効化を行うことができる。したがって、一つ錠前装置2003に対して、複数のユーザが合鍵を持つことができ、また、その合鍵を個々に無効化することもできる。従来の鍵では、鍵を紛失したり

、合鍵が返却されなかったりした場合、安全のために錠前装置を交換する必要があったが、本電子鍵システムによれば、電子鍵(ev)を格納した携帯電話2001を紛失したり、友人の携帯電話に発行した電子鍵(ev)が返却されなかったりしても、錠前装置2003側で電子鍵(ev)を無効化し、改めて、携帯電話2001に電子鍵(ev)を発行するといったことが可能となり、ユーザの利便性を向上させることができる。

【０２７０】

ネットワーク2004は、携帯電話の無線通信ネットワークとインターネットによって構成され、携帯電話2001とセンター2002との無線通信による通信を可能にする。携帯電話2001とセンター2002との通信では、常に、SSL(Secure Sockets Layer)やTLS(Transport Layer Security)などのセキュアセッションを確立され、通信データは暗号化されて伝送される。

【０２７１】

携帯電話2001と錠前装置2003とは、ローカルワイヤレス通信機能（赤外線通信、Bluetooth、無線ＬＡＮ、非接触ＩＣカードの無線通信など）を用いて、アドホックに接続して通信する。

【０２７２】

携帯電話2001には、電子鍵(ev)を管理するワレットアプリケーションが搭載されている。ワレットアプリケーションとしては、予めユーザが携帯電話2001にダウンロードしていた汎用のワレットアプリケーションでも、錠前装置2003を購入したユーザがセンター2002からダウンロードする専用のワレットアプリケーションでも良い。錠前装置2003を購入したユーザが、センター2002からワレットアプリケーションを携帯電話2001にダウンロードする手順については後で詳しく説明する。

【０２７３】

センター2002には、ワレットアプリケーションが管理されており、また、錠前装置2003には、電子鍵(ev)の暗号化されている部分を復号化する暗号鍵を生成するためのマスター鍵(Km)と、錠前装置2003の識別情報である錠前ＩＤと、錠前装置2003が電子鍵(ev)を発行する際の認証番号となる錠前番号(LN)などが管理されている。

【０２７４】

本電子鍵システムの錠前装置2003の内部構成は、基本的に第８の実施形態の場合と同じであり、図２１が錠前装置2003の内部構成を示すブロック図である。錠前装置2003は、物理的にロックの開閉を錠前機構部2111と、ユーザの操作を検出して錠前装置2003を起動する起動センサー2112と、ローカルワイヤレス通信Ｉ／Ｆ2113と、錠前装置2003の状態を示すＬＥＤ2114と、制御スイッチ2115と、それらを制御する制御部2110とによって構成され、制御部2110にはその他の部分を直接制御する制御回路の他に、セキュリティモジュール2100が組み込まれている。錠前装置2003がドアに取り付けられるタイプの場合には、外部からの悪戯等を防止するため、制御スイッチ2115はドアの内側に位置することが望ましい。

【０２７５】

ローカルワイヤレス通信Ｉ／Ｆ2113は、赤外線通信や、Bluetooth、無線ＬＡＮ、非接触ＩＣカードの無線通信などの通信Ｉ／Ｆであり、携帯電話とアドホックに接続して通信を行うためのものである。

【０２７６】

セキュリティモジュール2100は、マスター鍵(Km)を安全に管理し、電子鍵の認証処理を安全に行うためのデバイスであり、セキュリティモジュール2100は、ＣＰＵ2101と、ＲＯＭ2102と、ＲＡＭ2103と、ＥＥＰＲＯＭ2104と、コ・プロセッサ2105によって構成され、外部からの不正なアクセスを防止する耐タンパ機能を有している。

【０２７７】

ＥＥＰＲＯＭ2104には、図２６に示すように、錠前ＩＤ2601、錠前番号(LN) 2602、ワレットアプリURL 2603、マスター鍵(Km) 2604、および、鍵ＩＤリスト2605が格納されている。錠前ＩＤ2601は、錠前装置2003の識別情報であり、錠前番号(LN) 2602は、錠前装

置2003が電子鍵(ev)を発行する際にユーザの認証に用いる認証番号、ワレットアプリＵＲＬ2603は、この錠前装置2003の専用のワレットアプリケーションのＵＲＬ(Uniform Resource Locator)、マスター鍵(Km) 2604は、この錠前装置2003の電子鍵(ev)の暗号化されている部分を復号化する暗号鍵を生成するためのマスター鍵、鍵ＩＤリスト2605は、錠前装置2003が発行し、現在、有効な電子鍵(ev)の鍵ＩＤ（識別情報）のリストである。

【０２７８】

錠前番号(LN) 2602は、錠前装置2003が製造されたときに設定される番号であり、錠前装置2003を所有するユーザのみが知っている必要がある番号である。したがって、錠前装置2003が販売されている時には、錠前番号(LN)は見えない形で販売される。例えば、ユーザが錠前装置2003を購入し、付属のスクラッチカードを削ることによって初めて錠前番号(LN)がユーザに知らされるといった方法がとられる。

【０２７９】

また、セキュリティモジュール2100のＥＥＰＲＯＭ2104に格納されている情報へのアクセスは、ＣＰＵ2101によって制御されており、制御部2110のその他の制御回路から、錠前ＩＤ2601とワレットアプリＵＲＬ2603は読出しは出来るが、書き換えはできない。また錠前番号(LN)2602は読出しも書き換えも出来ない。マスター鍵(Km)2604は読出しと書き換えは出来ないが、セキュリティモジュール2100の内部で新たに鍵を生成して新しいマスター鍵(Km)に更新することが出来る。また、鍵ＩＤリスト2605は読出しと書き換えは出来ないが、鍵ＩＤの消去、および、電子鍵を発行することに新たに鍵ＩＤを追加することが出来るように制御されている。

【０２８０】

マスター鍵(Km)の更新や、鍵ＩＤの消去は、ユーザが、ＬＥＤ2115が示す錠前装置2003の状態を確認しながら、制御スイッチ2115を操作することによって行うことが出来る。マスター鍵(Km)を更新した場合、鍵ＩＤリスト2605は消去される。

【０２８１】

携帯電話2001は、ワレットアプリケーションが錠前装置2003から電子鍵(ev)を入手する機能を備えている以外は、第８の実施の形態で説明した携帯電話2001と同様のものであり、ローカルワイヤレス通信Ｉ／Ｆを備えており、携帯電話2001のワレットアプリケーションは、ローカルワイヤレス通信Ｉ／Ｆを介して錠前装置2003とアドホックに接続し、ワレットアプリケーションが管理している電子鍵(ev)を用いて電子鍵の認証処理を行う。したがって、ワレットアプリケーションが、携帯電話2001のメモリ（不揮発性メモリ）上に管理する情報については、ここでは説明を省略する。

【０２８２】

また、電子鍵(ev)のデータ構造も、基本的に第８の実施の形態の場合と同じであり、図２３は、本電子鍵システムにおける電子鍵(ev)のデータ構造を示している。ただし、署名情報2304は、電子鍵公開情報2301と、暗号化する前の電子鍵秘密情報2302及びバリュー認証情報2303とを連結したデータに対するハッシュ演算の結果とする。署名情報2304は、電子鍵の認証処理の際に、錠前装置2003側で暗号が復号化され、新たにハッシュ演算を行った結果と照合することによって、電子鍵(ev)が改ざんまたは偽造されていないことを検証するのに用いられる。

【０２８３】

次に、ユーザが錠前装置2003の制御スイッチ2115を操作してセンター2002から携帯電話2001にワレットアプリケーションをダウンロードする手順について説明する。図２７は、ワレットアプリケーションのダウンロードの手順を示している。まず、ユーザが錠前装置2003の制御スイッチ2115を操作して、ワレットアプリケーションをダウンロードする初期設定操作を行い(2700)、ユーザが錠前装置2003からのメッセージ受信を可能にする操作を携帯電話2001に対して行うと(2701)、携帯電話2001は錠前装置2003からナビゲーションメッセージを受信する(2702)。ナビゲーションメッセージには、ワレットアプリＵＲＬと錠前ＩＤが含まれている。

【０２８４】

ナビゲーションメッセージを受信した携帯電話2001は、ユーザにワレットアプリケーションをダウンロードするか問い合わせる画面を表示し(2703)、ユーザがワレットアプリケーションをダウンロードする操作を行うと(2704)、携帯電話2001は、ワレットアプリＵＲＬが示すセンター2002に対して、ワレットアプリダウンロード要求を送信する(2705)。ワレットアプリダウンロード要求には、錠前ＩＤが含まれている。

【０２８５】

ワレットアプリダウンロード要求を受信したセンター2002では、錠前ＩＤから錠前装置の種類を特定し(2706)、錠前装置2003に適したワレットアプリケーションを携帯電話2001に対して発行する(2707)。ワレットアプリケーションを受信した携帯電話2001は、ワレットアプリケーションをメモリに格納し(2708)、ダウンロードの完了を表示して(2709)、ワレットアプリケーションのダウンロードを完了する。

【０２８６】

次に、錠前装置2003から携帯電話2001に電子鍵(ev)を発行する手順について説明する。図２８は、錠前装置2003から携帯電話2001に電子鍵(ev)を発行する手順を示している。まず、ユーザが携帯電話2001のワレットアプリケーションを起動すると(2800)、メニュー画面が表示され(2801)、メニュー選択によってユーザが錠前装置の電子鍵の発行を要求する操作を行うと(2802)、錠前番号と、電子鍵(ev)に対応してユーザが設定するバリューパスワード(VPW: value password)を入力する画面が表示される(2803)。

【０２８７】

ユーザが錠前装置2003の錠前番号(LN')とバリューパスワード(VPW)を入力すると(2804)、携帯電話2001は、バリューパスワード(VPW)のハッシュ演算結果 Hash(VPW)をバリューパスワードの参照データとして携帯電話2001のメモリに格納し(2805)、さらに、錠前番号(LN')と時刻(T) とから、ユーザ識別情報 UID = Hash(LN'|| T) (※ ||はデータの連結を示す) を生成してメモリに格納する(2806)。この時、参照データHash(VPW)とユーザ識別情報 UID = Hash(LN'|| T)は、携帯電話2001のメモリ上の電子鍵リスト2204に、新しい電子鍵に関するデータとして、参照データとユーザ識別情報のフィールドにそれぞれ格納される。

【０２８８】

さらに、ユーザが錠前装置2003の制御スイッチ2115を操作して、錠前装置2003を、電子鍵を発行するモードにすると(2807)、錠前装置2003は、乱数R0を生成し(2808)、携帯電話2001に電子鍵発行チャレンジを送信する(2809)。電子鍵発行チャレンジは、携帯電話2001に対するチャレンジメッセージであり、その中には乱数R0が含まれている。この乱数R0はセキュリティモジュール2100から取得したもので、実際にはセキュリティモジュール2100のＣＰＵ2101が生成したものである。

【０２８９】

電子鍵発行チャレンジを受信した携帯電話2001は、バリューパスワード(VPW)とユーザ識別情報(UID)とから、バリュー認証情報 F(VPW) = Hash(VPW || UID) を生成し、さらに、錠前番号(LN')と乱数R0を連結してそのハッシュであるHash(LN'|| R0)を計算し(2810)、Hash(LN'|| R0)とバリュー認証情報 F(VPW)を含む電子鍵発行要求を錠前装置2003に送信する(2811)。

【０２９０】

電子鍵発行要求を受信した錠前装置2003は、受信したHash(LN'|| R0)とバリュー認証情報 F(VPW)をセキュリティモジュール2100に送り、電子鍵(ev)の生成処理をセキュリティモジュール2100に行わせる。セキュリティモジュール2100は、錠前番号(LN)と乱数R0を連結してそのハッシュHash(LN || R0)を計算し、受信したHash(LN'|| R0)と照合して、ユーザが錠前番号(LN)を知っている錠前装置2003の正しい所有者であることを認証する(2812)。

【０２９１】

ユーザが認証された場合 (Hash(LN'|| R0)がHash(LN || R0)と一致) 、セキュリティモジュール2100は、バリュー認証情報 F(VPW)をハッシュ演算し、マスター鍵Kmと連結して

、さらに、ハッシュ演算をして、電子鍵(ev)を暗号化する共通鍵暗号方式の暗号鍵Kk = Hash(Km || Hash(F(VPW)))を生成する(2813)。さらに、セキュリティモジュール2100は、電子鍵(ev)の電子鍵公開情報及び電子鍵秘密情報を生成し、受信したバリュー認証情報 F(VPW)と暗号鍵Kkとを用いて、図２３に示したデータ構造を持つ電子鍵(ev)を生成して、生成した電子鍵(ev) の鍵ＩＤを鍵ＩＤリスト2605に登録する(2814)。電子鍵(ev)を生成する際、セキュリティモジュール2100は、電子鍵(ev)にユニークな鍵ＩＤを割り当てる。

【０２９２】

ユーザが認証されなかった場合（Hash(LN' || R0)がHash(LN || R0)と不一致）、セキュリティモジュール2100は錠前装置2003に対しエラーを返し、さらに、錠前装置2003から携帯電話2001にエラーメッセージが送られ、電子鍵の発行処理を終了する（図には記載していない）。

【０２９３】

生成された電子鍵(ev)は、携帯電話2001に送信されて(2815)、電子鍵(ev)は、携帯電話のメモリに格納され(2816)、携帯電話2001が発行処理の完了を表示して(2817)、電子鍵の発行処理を完了する。この時、電子鍵(ev)は、携帯電話2001のメモリ上の電子鍵リスト2204に、新しい電子鍵として格納される。また、プロパティにはデフォルトのプロパティが設定され、デフォルトの設定では、電子鍵の認証処理の際に使用される音は設定されていない。

【０２９４】

また、図２８のステップ(2804)において、ユーザが電子鍵の認証処理の安全性よりも操作性を優先する判断をして、バリューパスワードを設定しなかった場合、携帯電話2001は、ステップ(2805)では、バリューパスワード(VPW)のハッシュ演算は行わず、電子鍵リスト2204の参照データのフィールドには、ヌルが設定してバリューパスワード(VPW)が設定されていないことを示し、ステップ(2810)では、ユーザ識別情報(UID)をハッシュ演算してバリュー認証情報 F(VPW) = Hash(UID)を生成する。

【０２９５】

ワレットアプリケーションを終了すると、ユーザが入力した錠前番号とバリューパスワード(VPW)とバリュー認証情報 F(VPW)は携帯電話2001のメモリから消去される。携帯電話のメモリに保持されている参照データは、バリューパスワードをハッシュ演算したものなので、仮に、携帯電話が第三者に盗まれて、内部のメモリの内容が解析されたとしても、バリューパスワードが知られる心配が無い。

【０２９６】

次に、電子鍵(ev)を用いて、錠前装置2003との間で認証処理を行い、錠前装置2003を開錠（または施錠）する手順について説明する。図２９は、本実施形態における電子鍵(ev)を用いた認証処理の手順を示している。まず、ユーザが、錠前装置2003が取り付けられている扉のハンドルに手をかけるなど、錠前装置2003を起動にさせる操作(2900)を行うと、錠前装置2003の起動センサー2112がそれを検出して錠前装置2003を起動し、錠前装置2003は、チャレンジ情報として乱数Rを生成する(2901)。この乱数Rはセキュリティモジュール2100から取得したもので、実際にはセキュリティモジュール2100のＣＰＵ2101が生成したものである。ユーザが錠前装置2003からのメッセージ受信を可能にする操作を行うと(2902)、携帯電話2001は錠前装置2003から電子鍵提示要求を受信する(2903)。電子鍵提示要求には、錠前ＩＤと乱数Rが含まれている。

【０２９７】

電子鍵提示要求を受信した携帯電話2001では、ワレットアプリケーションが起動され、電子鍵を使用するかをユーザに問い合わせるダイアログが表示される(2904)。この時、携帯電話2001は、受信した錠前ＩＤと電子鍵リスト2205とを照合して、その錠前装置2003の電子鍵をユーザに提示する。該当する電子鍵がなかった場合には、該当する電子鍵がないことをユーザに示す（図には記載していない）。

【０２９８】

ユーザが電子鍵使用操作(2905)を行うと、電子鍵に対応するバリューパスワードを入力

する画面が表示される(2906)。ユーザがバリューパスワード(VPW')を入力すると(2907)、携帯電話2001は、バリューパスワード(VPW')のハッシュHash(VPW')を計算し、電子鍵リスト2204上の対応する電子鍵の参照データのHash(VPW)と照合してユーザを認証する(2908)。参照データと一致しなかった場合にはエラーを表示し（図には記載していない）、参照データと一致した場合には、携帯電話2001は、ユーザが入力したバリューパスワード(VPW')を用いて、バリュー認証情報 F(VPW')= Hash(VPW'|| UID) 及び 、バリュー認証情報 F(VPW')と乱数Rとの連結のハッシュ Hash(F(VPW') || R)、バリュー認証情報のハッシュ Hash(F(VPW'))をそれぞれ計算し(2909)、錠前装置2003に電子鍵を提示するメッセージとして、電子鍵(ev)と共にHash(F(VPW') || R)とHash(F(VPW'))を送信する(2910)。この時、電子鍵(ev)の表示用情報2305の部分は送信されない。

【０２９９】

錠前装置2003は、まず、受信した電子鍵(ev)の電子鍵公開情報2301の内容の有効性を検証（錠前ＩＤと有効期限の検証）した後、受信した電子鍵(ev)とHash(F(VPW') || R)とHash(F(VPW'))を、セキュリティモジュール2100に送り、電子鍵(ev)とユーザのオフライン認証をセキュリティモジュール2100に行わせる。電子鍵公開情報2301の内容の有効性の検証（錠前ＩＤと有効期限の検証）においてエラーが検出された場合、錠前装置2003から携帯電話2001にエラーメッセージが送られ、電子鍵の認証処理を終了する（図には記載していない）。

【０３００】

セキュリティモジュール2100は、まず、電子鍵(ev)の電子鍵公開情報2301の中の鍵ＩＤと鍵ＩＤリスト2605と照合して、電子鍵(ev)が鍵ＩＤリスト2605に登録されている有効な電子鍵であることを検証する(2911)。電子鍵(ev)が鍵ＩＤリスト2605に登録されていた場合、セキュリティモジュール2100は、バリュー認証情報のハッシュ Hash(F(VPW'))とマスター鍵Kmの連結のハッシュを計算して電子鍵のセキュリティ情報2300の部分を復号化する共通鍵暗号方式の復号鍵Kk'= Hash(Km || Hash(F(VPW')))を生成し、コ・プロセッサ2105を用いて電子鍵のセキュリティ情報2300を復号化する(2912)。

【０３０１】

さらに、セキュリティモジュール2100は、復号化したセキュリティ情報2300からバリュー認証情報2303F(VPW)を取り出し、乱数Rとの連結のハッシュ Hash(F(VPW) || R)を計算し、携帯電話2001から受信したHash(F(VPW') || R)と照合し、一致していた場合、ユーザが電子鍵の正しい所有者であると認証する(2913)。さらに、セキュリティモジュール2100は、電子鍵(ev)の電子鍵公開情報2301と、暗号を復号化した電子鍵秘密情報2302及びバリュー認証情報2303とを連結したデータに対するハッシュを計算し、署名情報2304と照合して電子鍵(ev)が改ざんまたは偽造されていないことを検証する(2914)。

【０３０２】

電子鍵(ev)が鍵ＩＤリスト2605に登録されていなかった場合、または、Hash(F(VPW) || R)とHash(F(VPW') || R)とが一致しなかった場合、または、署名情報の検証(2913)においてエラーが検出された場合には、セキュリティモジュール2100は錠前装置2003に対しエラーを返し、さらに、錠前装置2003から携帯電話2001にエラーメッセージが送られ、電子鍵の認証処理を終了する（図には記載していない）。

【０３０３】

署名情報の検証(2914)においてエラーが検出されなかった場合、つまり、電子鍵(ev)の有効性が検証された場合、セキュリティモジュール2100は錠前装置2003に対してオフライン認証の完了を示し、錠前装置2003は、携帯電話2001に認証結果を送信して(2915)、認証処理を完了し、認証結果を受信した携帯電話2001は、完了を表示して(2917)、電子鍵の認証処理を完了する。

【０３０４】

また、錠前装置2003は、制御部2106が錠前機構部2107を制御して錠前装置2103のロックを開錠（または施錠）し、錠前装置2003での電子鍵の認証処理を完了する(2916)。

【０３０５】

また、携帯電話2001は、電子鍵の認証処理を完了すると、その使用した電子鍵のプロパティに基づいて、認証処理が完了したことを示す。また、携帯電話2001は、錠前装置2003からエラーメッセージが送られて電子鍵の認証処理を終了した場合も、同様にして、その使用した電子鍵のプロパティに基づいて、電子鍵の認証処理が失敗したことを示す。

【０３０６】

また、電子鍵使用操作(2905)において、バリューパスワードが設定されていない電子鍵の使用をユーザが選択された場合には、図２９のステップ(2906)、ステップ(2907)、ステップ(2908)の処理は行わず、携帯電話2001はステップ(2909)の処理に進み、ユーザ識別情報(UID)をハッシュ演算してバリュー認証情報 F(VPW') = Hash(UID)を計算する。

【０３０７】

また、この電子鍵の認証処理の場合も、ワレットアプリケーションを終了すると、ユーザが入力したバリューパスワードとバリュー認証情報はメモリから消去される。携帯電話2001と錠前装置2003との間で交換されるデータの中で、認証処理に用いられるデータは、すべて、ハッシュ演算、または、暗号化されたデータであるため、仮に、第三者によって携帯電話2001と錠前装置2003との間の通信が盗聴されたとしても、その盗聴したデータを用いて、成りすましを行うことは出来ない。

【産業上の利用可能性】

【０３０８】

本発明に係る電子バリューの認証方式と認証システムと装置は、耐タンパ機能のない携帯端末を利用して、安全な認証処理を行うことができるなどの効果を有し、クレジットカードやデビットカード、会員証、ＩＤカード、チケットなどを電子情報化した電子バリューをユーザの携帯端末に格納し、ユーザが、それらの正しい所有者であることを認証することで、それぞれに対応する物やサービスがユーザに提供されるサービス等に有用である。

【図面の簡単な説明】

【０３０９】

【図１】本発明の第５の実施の形態における電子クレジットのダウンロード処理のフロー図

【図２】本発明の第５の実施の形態における電子クレジット決済処理のフロー図

【図３】本発明の第５の実施の形態における電子クレジットのデータ構造を示す模式図

【図４】本発明の第６の実施の形態における電子クレジット決済システムのブロック図

【図５】本発明の第６の実施の形態におけるクレジット決済端末のブロック図

【図６】本発明の第６の実施の形態におけるセキュリティカードのフラッシュメモリ部に格納される情報を示す模式図

【図７】本発明の第６の実施の形態における携帯電話のメモリ（不揮発性メモリ）に格納されるワレットアプリケーションが管理する情報を示す模式図

【図８】本発明の第６の実施の形態における電子クレジットのデータ構造を示す模式図

【図９】本発明の第６の実施の形態における電子クレジットのダウンロード処理のフロー図

【図１０】本発明の第６の実施の形態における電子クレジット決済処理のフロー図

【図１１】本発明の第６の実施の形態における電子チケット決済処理のフロー図

【図１２】本発明の第７の実施の形態における電子チケットシステムのブロック図

【図１３】本発明の第７の実施の形態における改札装置のブロック図

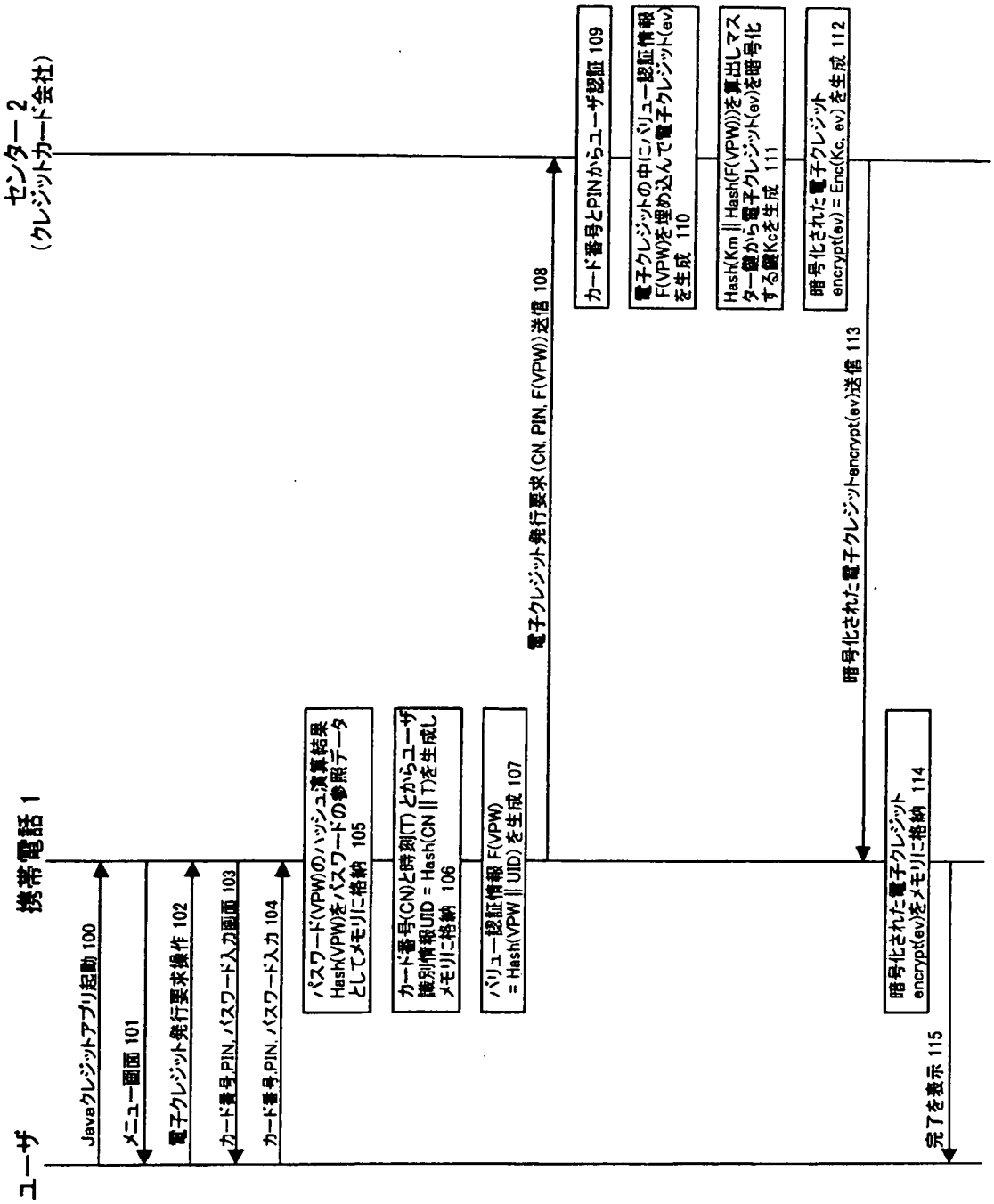
【図１４】本発明の第７の実施の形態におけるセキュリティモジュールのフラッシュメモリ部に格納される情報を示す模式図

【図１５】本発明の第７の実施の形態における携帯電話のメモリ（不揮発性メモリ）に格納されるワレットアプリケーションが管理する情報を示す模式図

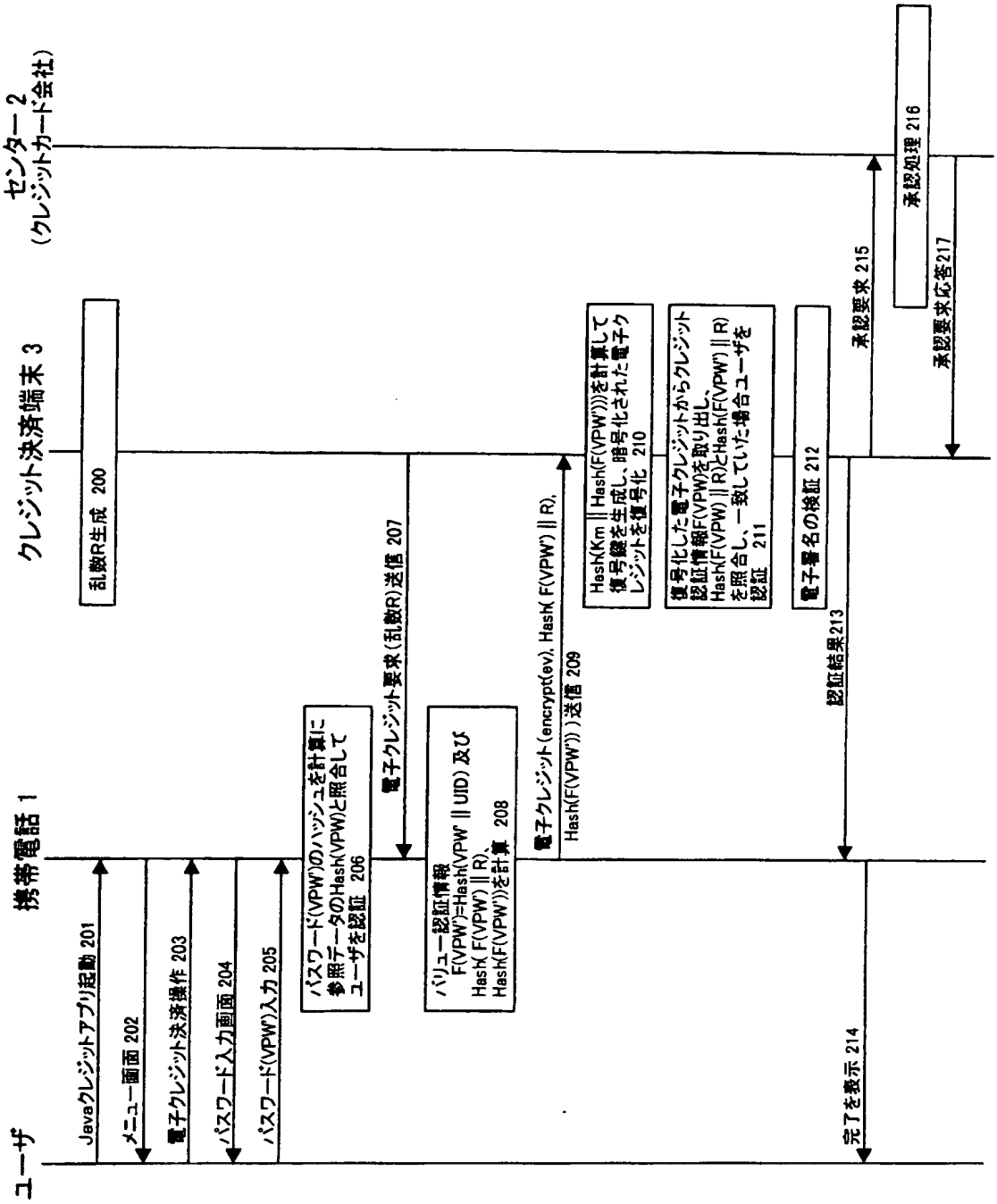
【図１６】本発明の第７の実施の形態における電子チケットのデータ構造を示す模式図
【図１７】本発明の第７の実施の形態における電子チケットのダウンロード処理のフロー図
【図１８】本発明の第７の実施の形態における電子チケット改札処理のフロー図
【図１９】本発明の第７の実施の形態における電子チケット改札処理のフロー図
【図２０】本発明の第８の実施の形態及び第９の実施の形態における電子鍵システムのブロック図
【図２１】本発明の第８の実施の形態及び第９の実施の形態における錠前装置のブロック図
【図２２】本発明の第８の実施の形態及び第９の実施の形態における携帯電話のメモリ（不揮発性メモリ）に格納されるワレットアプリケーションが管理する情報を示す模式図
【図２３】本発明の第８の実施の形態及び第９の実施の形態における電子鍵のデータ構造を示す模式図
【図２４】本発明の第８の実施の形態における電子鍵のダウンロード処理のフロー図
【図２５】本発明の第８の実施の形態における電子鍵の認証処理のフロー図
【図２６】本発明の第９の実施の形態におけるセキュリティモジュールのＥＥＰＲＯＭに格納される情報を示す模式図
【図２７】本発明の第９の実施の形態におけるワレットアプリケーションのダウンロード処理のフロー図
【図２８】本発明の第９の実施の形態における電子鍵の発行処理のフロー図
【図２９】本発明の第９の実施の形態における電子鍵の認証処理のフロー図
【図３０】本発明の第５の実施の形態における電子クレジット決済システムのブロック図
【図３１】本発明の概要を示す図
【図３２】認証要求装置と認証装置との処理のシーケンス図
【図３３】暗号化第一情報、第二情報、第一情報と第二情報とが所定の関係にあるかどうかの判断の条件の一例図
【図３４】本発明の第１の実施形態に係る認証要求装置の機能ブロック図
【図３５】暗号化第一情報の一例図
【図３６】本発明の第１の実施形態に係る認証装置の機能ブロック図
【図３７】本発明の第１の実施形態の処理のフロー図
【図３８】本発明の第２の実施形態に係る認証要求装置の機能ブロック図
【図３９】本発明の第３の実施形態に係る認証要求装置の機能ブロック図
【図４０】本発明の第３の実施形態の処理のフロー図
【図４１】本発明の第４の実施形態の情報関連付装置の機能ブロック図
【図４２】本発明の第４の実施形態の情報関連付装置の処理のフロー図
【図４３】本発明の実施例の一例図
【図４４】図４３における各データの関係を示す図

【符号の説明】
【０３１０】
1,401,1201,2001　携帯電話
2,402,1202,2002　センター
3,403　クレジット決済端末
404　アクワイアラ
405,1204,2004　ネットワーク
406　ネットワーク
1203　改札装置
2003　錠前装置

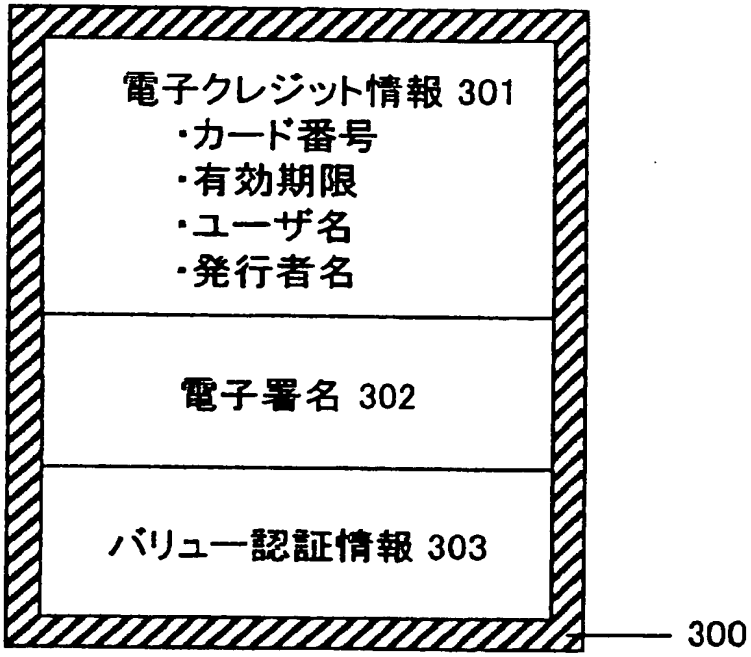
【書類名】図面
【図１】


ユーザ
携帯電話 1
センター 2
(クレジットカード会社)
Javaクレジットアプリ起動 100
メニュー画面 101
電子クレジット発行要求操作 102
カード番号,PIN,パスワード入力画面 103
カード番号,PIN,パスワード入力 104
パスワード(VPW)のハッシュ演算結果Hash(VPW)をパスワードの参照データとしてメモリに格納 105
カード番号(CN)と時刻(T)とからユーザ識別情報UID = Hash(CN || T)を生成しメモリに格納 106
バリュー認証情報 F(VPW) = Hash(VPW || UID)を生成 107
電子クレジット発行要求(CN, PIN, F(VPW))送信 108
カード番号とPINからユーザ認証 109
電子クレジットの中にバリュー認証情報F(VPW)を埋め込んで電子クレジット(ev)を生成 110
Hash(Km || Hash(F(VPW)))を算出しマスター鍵から電子クレジット(ev)を暗号化する鍵Kcを生成 111
暗号化された電子クレジット encrypt(ev) = Enc(Kc, ev)を生成 112
暗号化された電子クレジットencrypt(ev)送信 113
暗号化された電子クレジットencrypt(ev)をメモリに格納 114
完了を表示 115

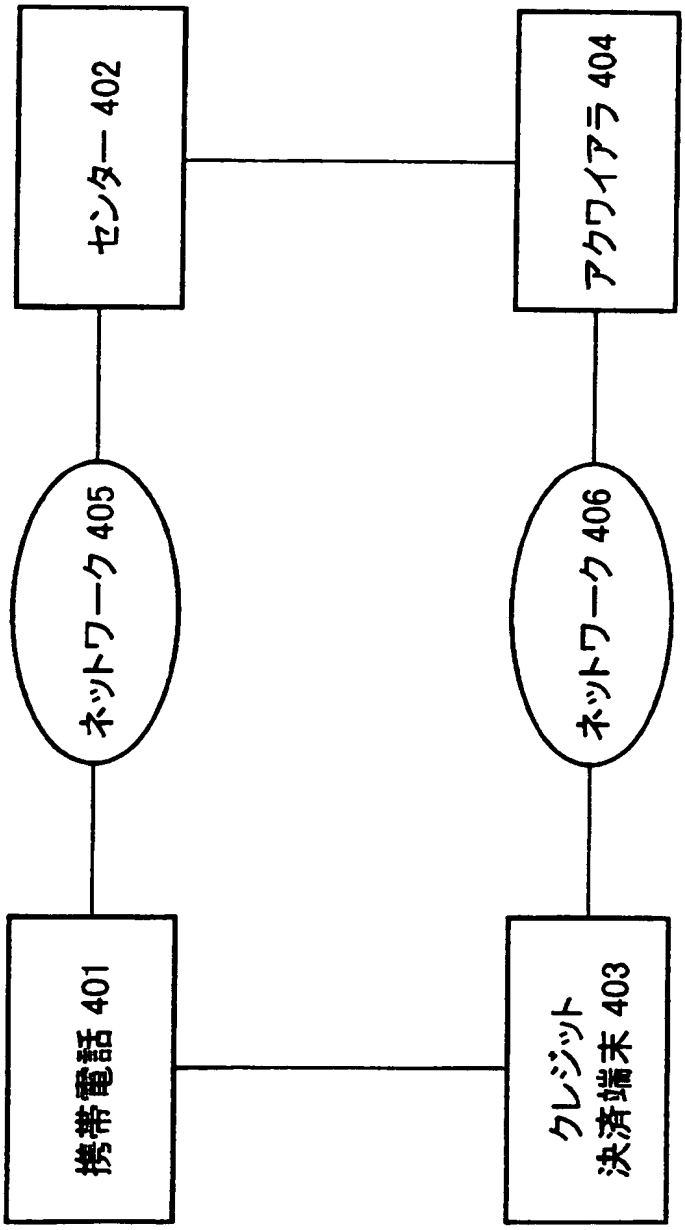
【図２】


ユーザ
携帯電話 1
クレジット決済端末 3
センター 2
(クレジットカード会社)
Javaクレジットアプリ起動 201
メニュー画面 202
電子クレジット決済操作 203
パスワード入力画面 204
パスワード(VPW')入力 205
パスワード(VPW')のハッシュを計算に
参照データのHash(VPW)と照合して
ユーザを認証 206
乱数R生成 200
電子クレジット要求(乱数R)送信 207
バリュー認証情報
F(VPW')=Hash(VPW' || R),
Hash(F(VPW') || R),
Hash(F(VPW'))を計算 208
電子クレジット(encrypt(ev), Hash(F(VPW') || R),
Hash(F(VPW')))送信 209
Hash(Km || Hash(F(VPW')))を計算して
復号鍵を生成し、暗号化された電子ク
レジットを復号化 210
復号化した電子クレジットからクレジット
認証情報F(VPW)を取り出し、
Hash(F(VPW) || R)とHash(F(VPW') || R)
を照合し、一致していた場合ユーザを
認証 211
電子署名の検証 212
認証結果213
完了を表示 214
承認要求 215
承認処理 216
承認要求応答217

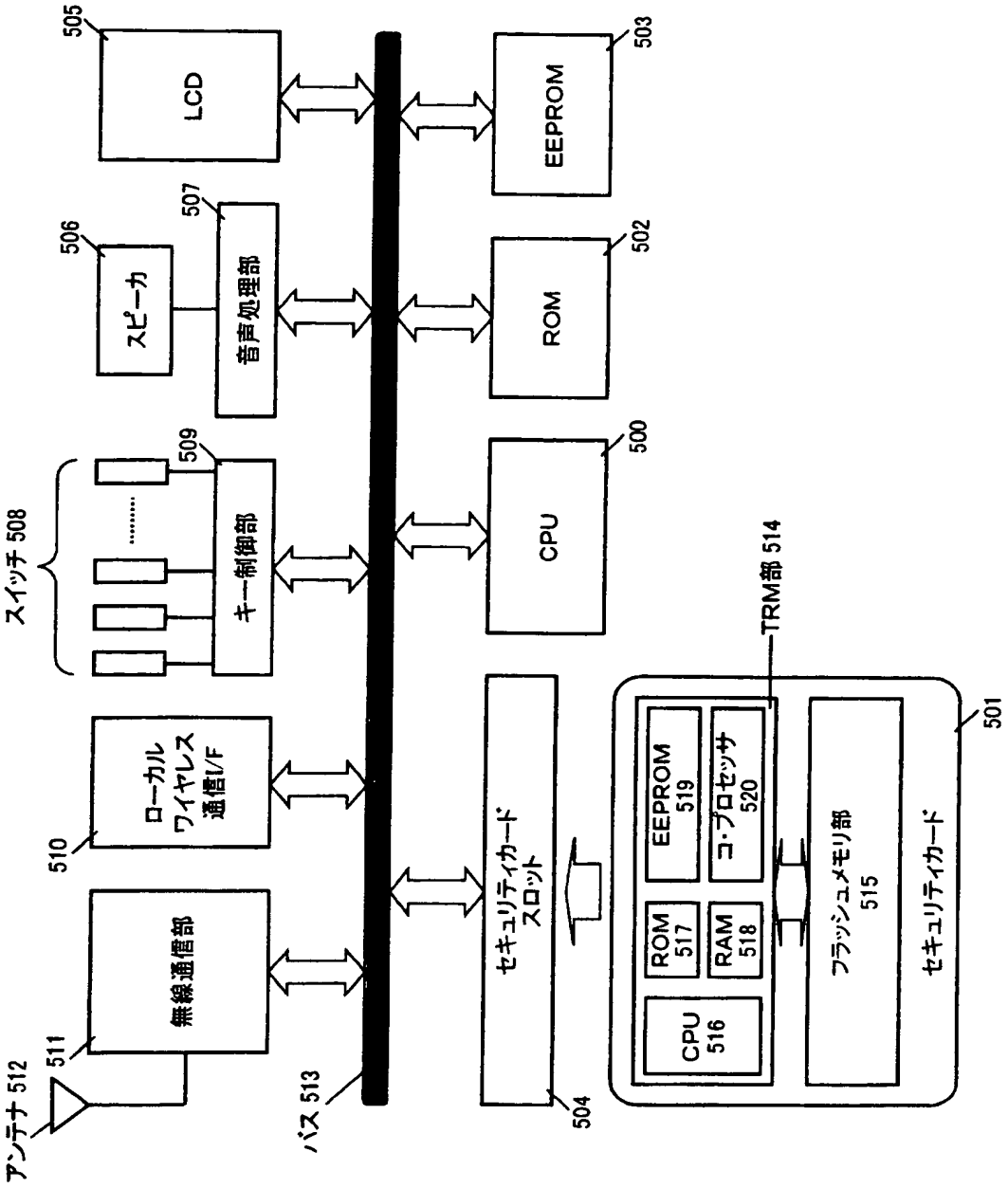
【図３】


電子クレジット情報 301
・カード番号
・有効期限
・ユーザ名
・発行者名
電子署名 302
バリュー認証情報 303
300

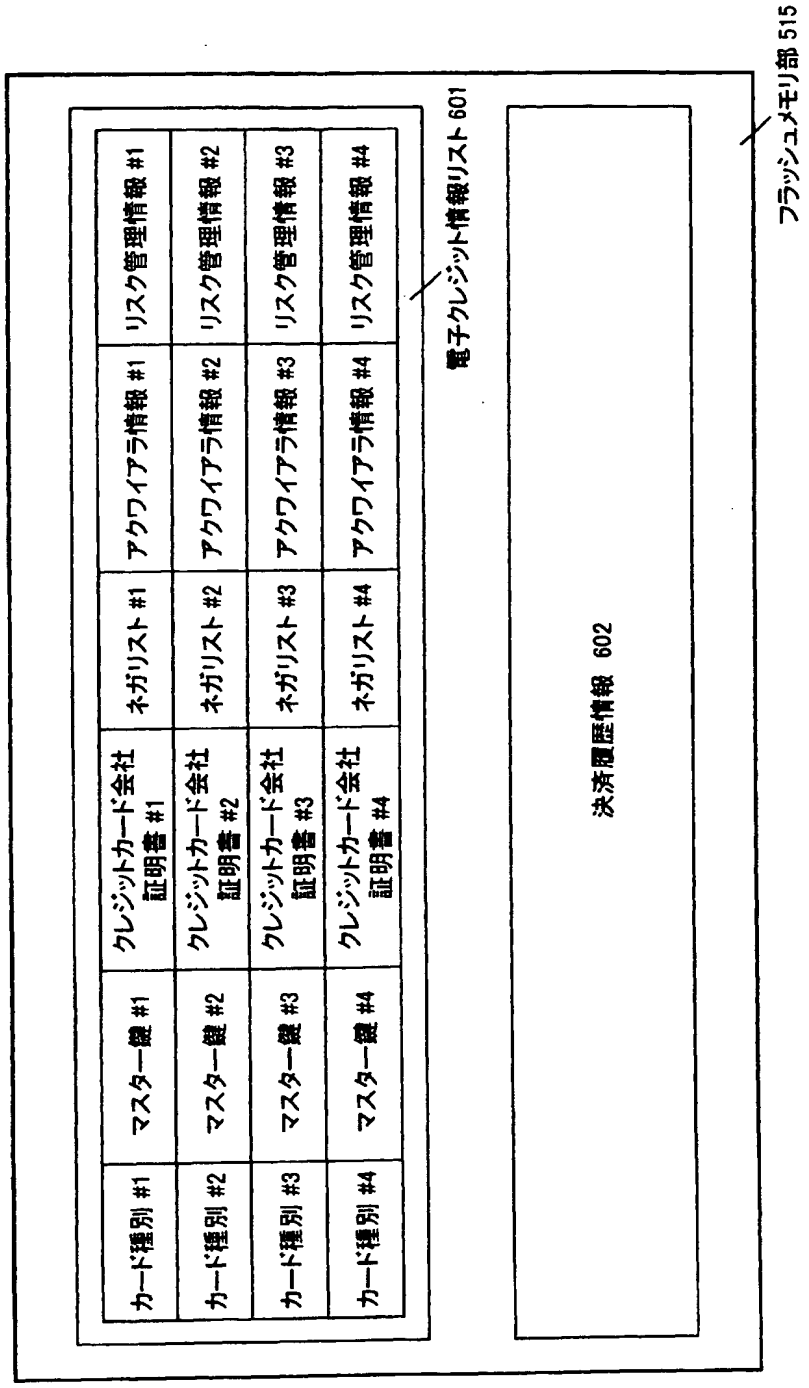
【図４】


センター 402
アクワイアラ 404
ネットワーク 405
ネットワーク 406
携帯電話 401
クレジット
決済端末 403

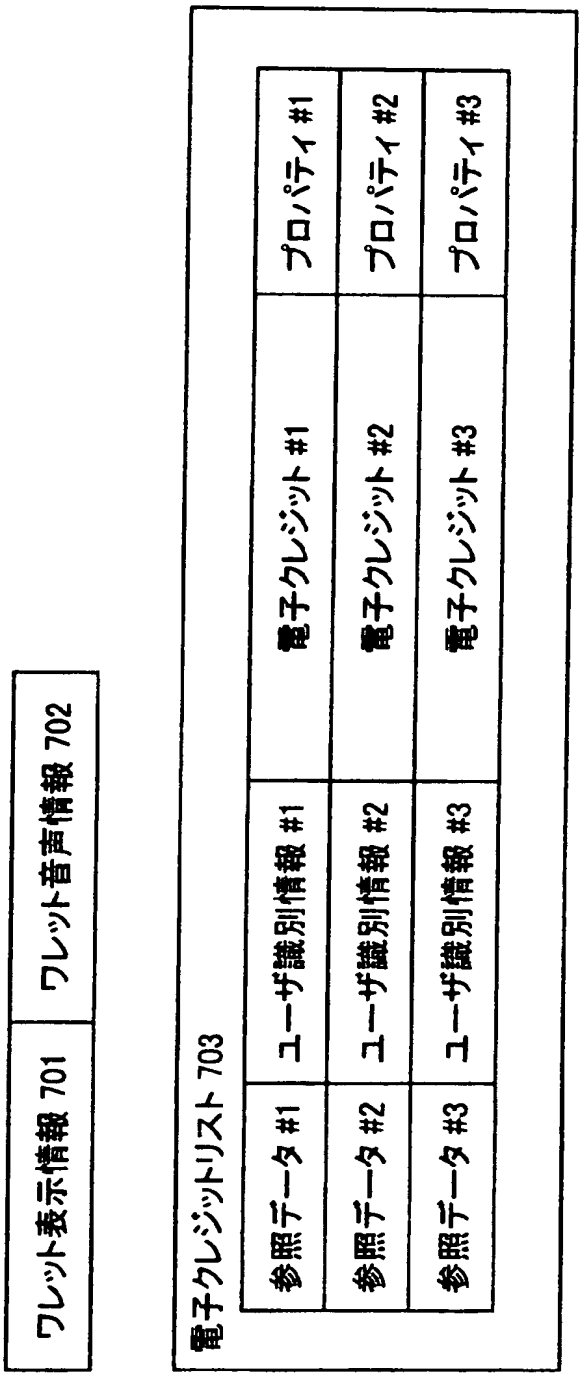
【図５】


505
LCD
503
EEPROM
507
506
スピーカ
音声処理部
502
ROM
509
スイッチ 508
キー制御部
500
CPU
TRM部 514
510
ローカル
ワイヤレス
通信I/F
セキュリティカード
スロット
501
EEPROM
519
ユ・プロセッサ
520
ROM
517
RAM
518
CPU
516
フラッシュメモリ部
515
セキュリティカード
511
無線通信部
アンテナ 512
バス 513
504

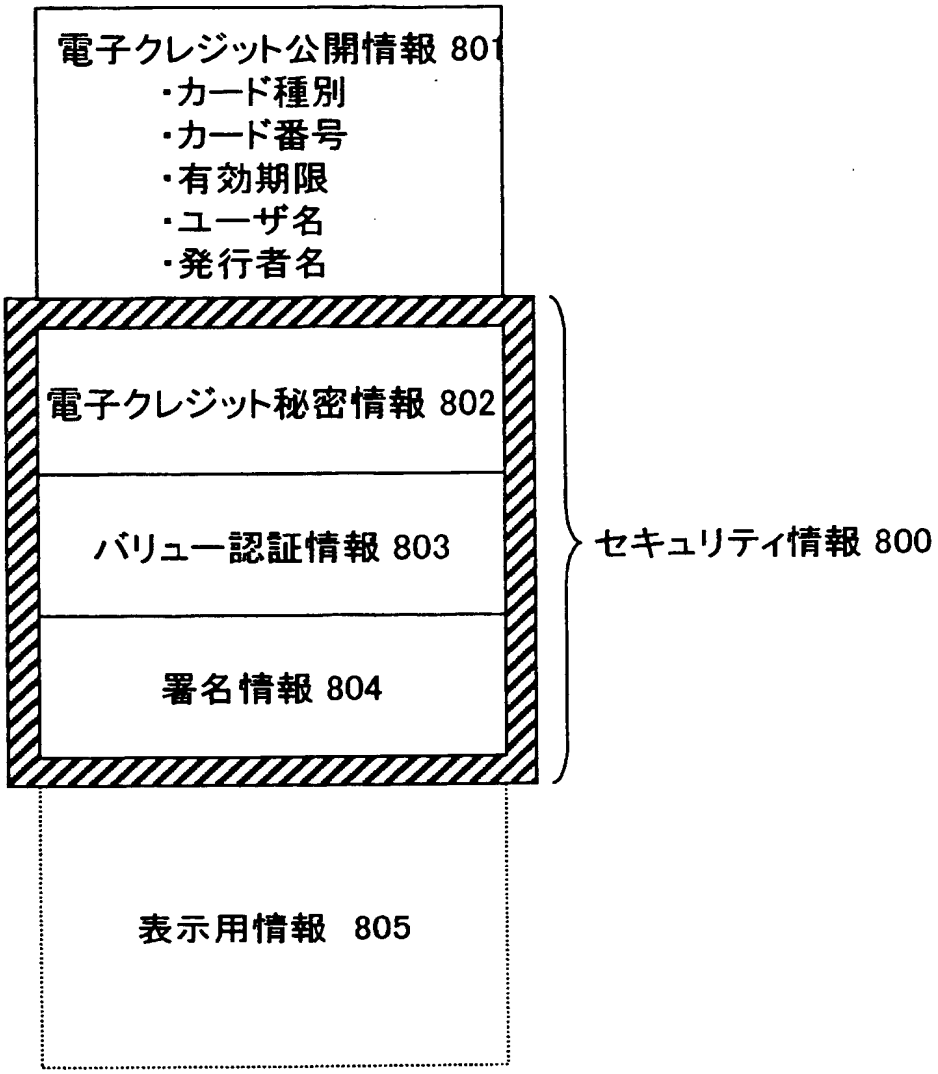
【図６】


フラッシュメモリ部 515
電子クレジット情報リスト 601
決済履歴情報 602
カード種別 #1
マスター鍵 #1
クレジットカード会社証明書 #1
ネガリスト #1
アクワイアラ情報 #1
リスク管理情報 #1
カード種別 #2
マスター鍵 #2
クレジットカード会社証明書 #2
ネガリスト #2
アクワイアラ情報 #2
リスク管理情報 #2
カード種別 #3
マスター鍵 #3
クレジットカード会社証明書 #3
ネガリスト #3
アクワイアラ情報 #3
リスク管理情報 #3
カード種別 #4
マスター鍵 #4
クレジットカード会社証明書 #4
ネガリスト #4
アクワイアラ情報 #4
リスク管理情報 #4

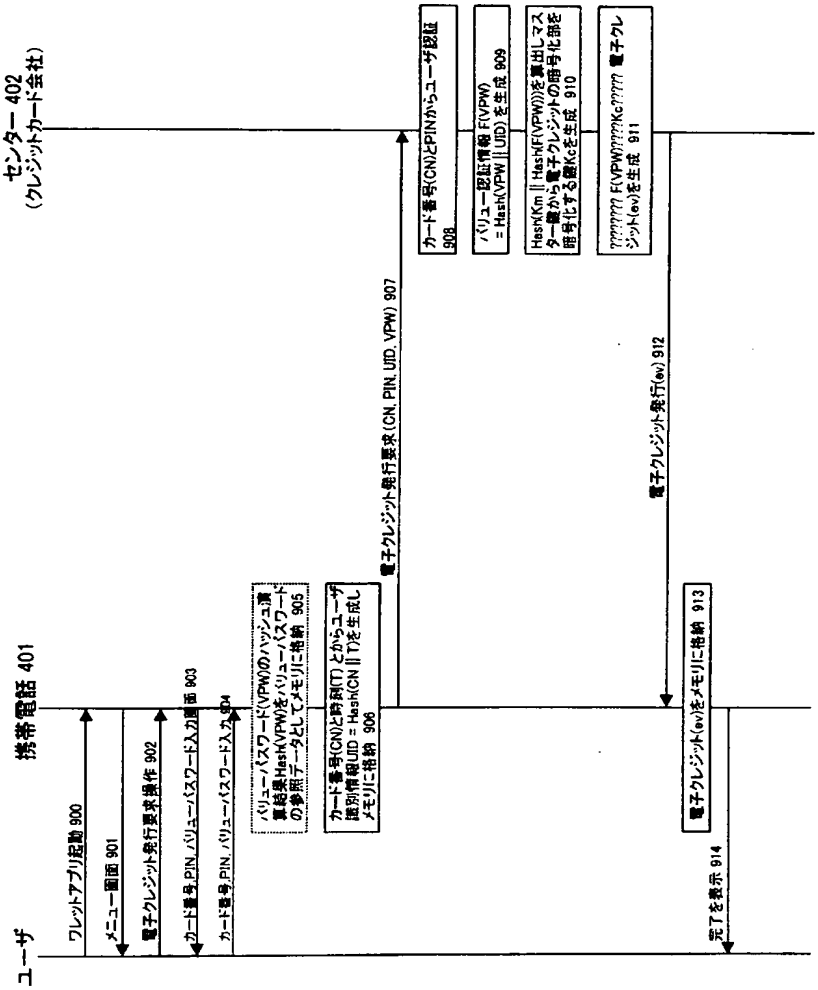
【図７】


ウレット表示情報 701
ウレット音声情報 702
電子クレジットリスト 703
参照データ #1
ユーザ識別情報 #1
電子クレジット #1
プロパティ #1
参照データ #2
ユーザ識別情報 #2
電子クレジット #2
プロパティ #2
参照データ #3
ユーザ識別情報 #3
電子クレジット #3
プロパティ #3

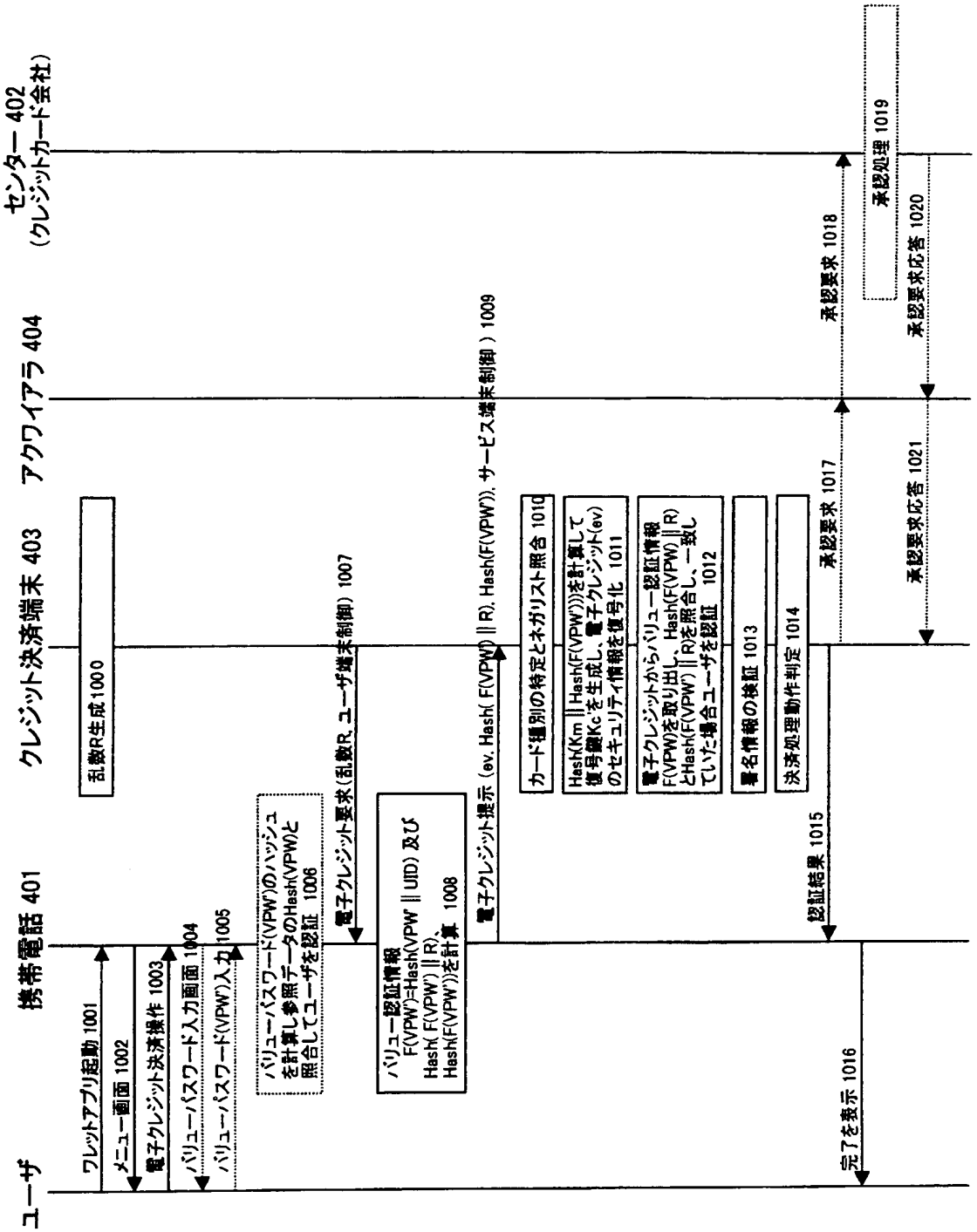
【図８】


電子クレジット公開情報 801
・カード種別
・カード番号
・有効期限
・ユーザ名
・発行者名
電子クレジット秘密情報 802
バリュー認証情報 803
署名情報 804
セキュリティ情報 800
表示用情報　805

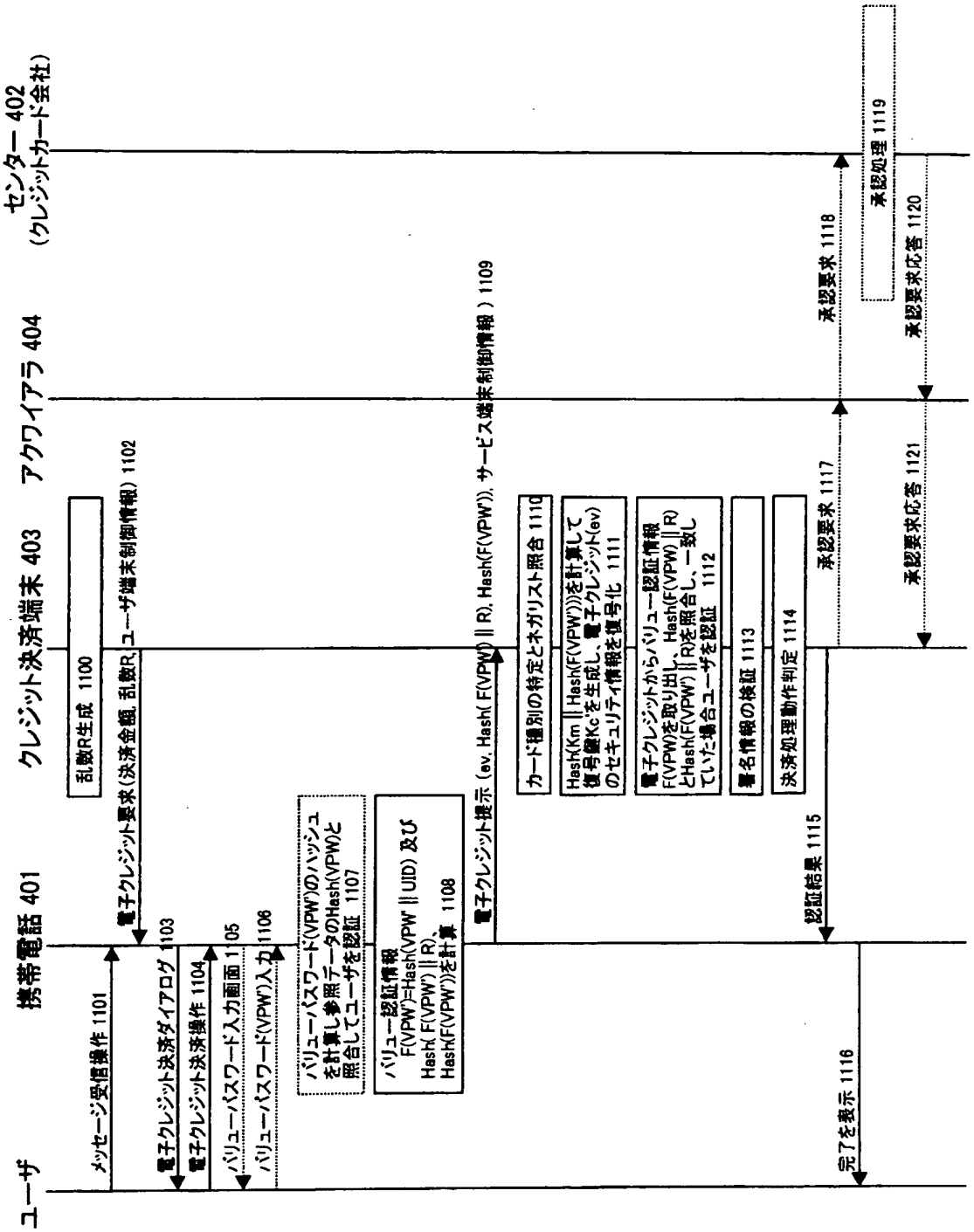
【図９】


センター 402
(クレジットカード会社)
携帯電話 401
ユーザ
ウレットアプリ起動 900
メニュー画面 901
電子クレジット発行要求操作 902
カード番号,PIN,バリューパスワード入力画面 903
カード番号,PIN,バリューパスワード入力 904
バリューパスワード(VPW)のハッシュ値算出結果Hash(VPW)をバリューパスワードの参照データとしてメモリに格納 905
カード番号(CN)と時刻(T)とからユーザ識別情報(UID = Hash(CN || T)を生成しメモリに格納 906
電子クレジット発行要求(CN, PIN, UID, VPW) 907
カード番号(CN)とPINからユーザ認証 908
バリュー認証情報 F(VPW) = Hash(VPW || UID) を生成 909
Hash(Km || Hash(F(VPW))を算出しマスター鍵から電子クレジットの暗号化部を暗号化する鍵Kcを生成 910
??????? F(VPW)?????Kc????? 電子クレジット(ev)を生成 911
電子クレジット発行(ev) 912
電子クレジット(ev)をメモリに格納 913
完了を表示 914

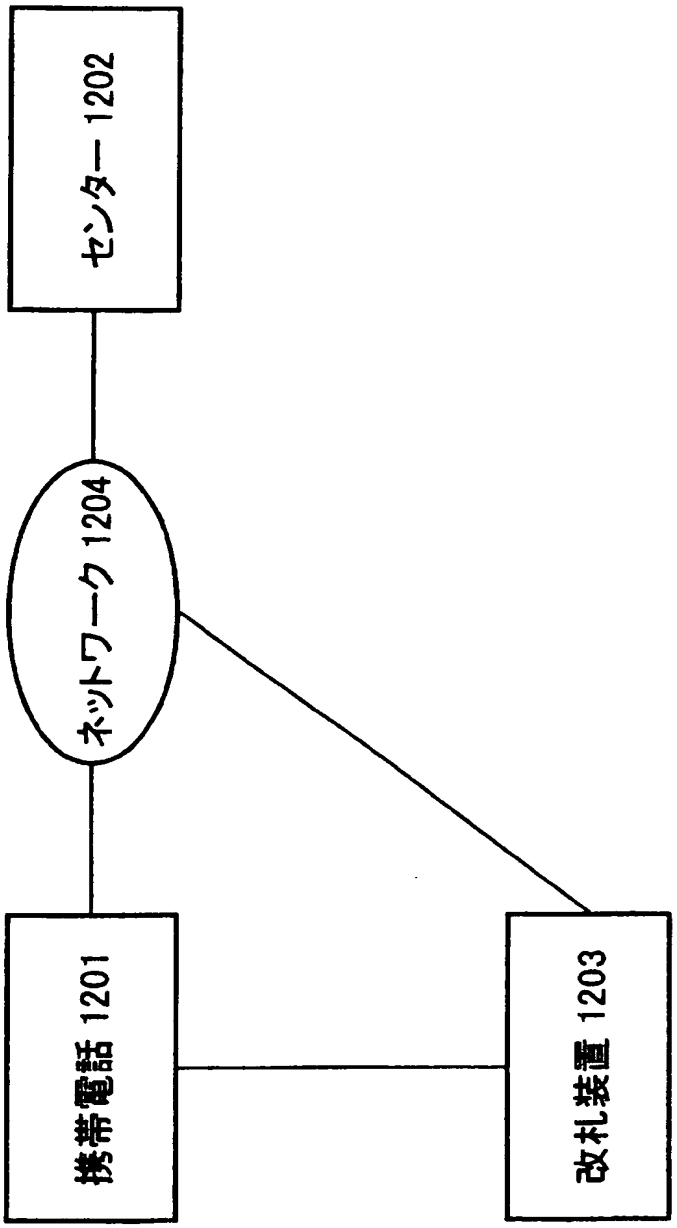
【図１０】


ユーザ
携帯電話 401
クレジット決済端末 403
アクワイアラ 404
センター 402
(クレジットカード会社)
ウレットアプリ起動 1001
メニュー画面 1002
電子クレジット決済操作 1003
バリューパスワード入力画面 1004
バリューパスワード(VPW')入力 1005
乱数R生成 1000
バリューパスワード(VPW')のハッシュを計算し参照データのHash(VPW)と照合してユーザを認証 1006
電子クレジット要求(乱数R, ユーザ端末制御) 1007
バリュー認証情報 F(VPW')=Hash(VPW' || UID) 及び Hash(F(VPW') || R), Hash(F(VPW'))を計算 1008
電子クレジット提示 (ev, Hash(F(VPW') || R), Hash(F(VPW')), サービス端末制御) 1009
カード種別の特定とネガリスト照合 1010
Hash(Km || Hash(F(VPW')))を計算して復号鍵Kcを生成し、電子クレジット(ev)のセキュリティ情報を復号化 1011
電子クレジットからバリュー認証情報 F(VPW)を取り出し、Hash(F(VPW) || R)とHash(F(VPW') || R)を照合し、一致していた場合ユーザを認証 1012
署名情報の検証 1013
決済処理動作判定 1014
認証結果 1015
完了を表示 1016
承認要求 1017
承認要求 1018
承認処理 1019
承認要求応答 1020
承認要求応答 1021

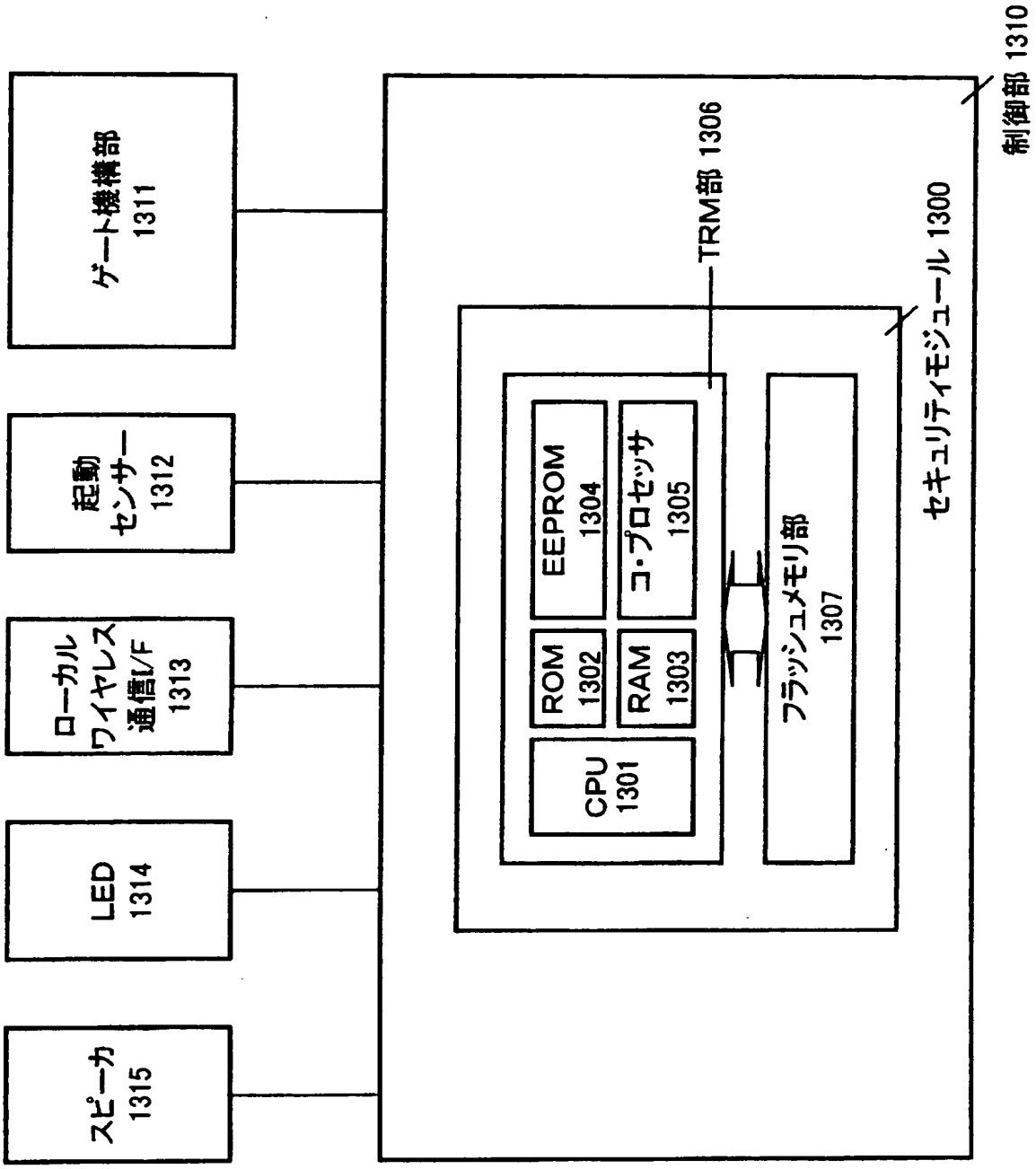
【図１１】


ユーザ
携帯電話 401
クレジット決済端末 403
アクワイアラ 404
センター 402
(クレジットカード会社)
メッセージ受信操作 1101
乱数R生成 1100
電子クレジット要求(決済金額, 乱数R, ユーザ端末制御情報) 1102
電子クレジット決済ダイアログ 1103
電子クレジット決済操作 1104
パリューパスワード入力画面 1105
パリューパスワード(VPW')入力 1106
パリューパスワード(VPW')のハッシュを計算し参照データのHash(VPW)と照合してユーザを認証 1107
パリュー認証情報 F(VPW')=Hash(VPW' || UID) 及び Hash(F(VPW') || R), Hash(F(VPW'))を計算 1108
電子クレジット提示 (ev, Hash(F(VPW') || R), Hash(F(VPW')), サービス端末制御情報) 1109
カード種別の特定とネガリスト照合 1110
Hash(Km || Hash(F(VPW')))を計算して復号鍵Kcを生成し、電子クレジット(ev)のセキュリティ情報を復号化 1111
電子クレジットからパリュー認証情報 F(VPW)を取り出し、Hash(F(VPW) || R)とHash(F(VPW') || R)を照合し、一致していた場合ユーザを認証 1112
署名情報の検証 1113
決済処理動作判定 1114
認証結果 1115
完了を表示 1116
承認要求 1117
承認要求 1118
承認処理 1119
承認要求応答 1120
承認要求応答 1121

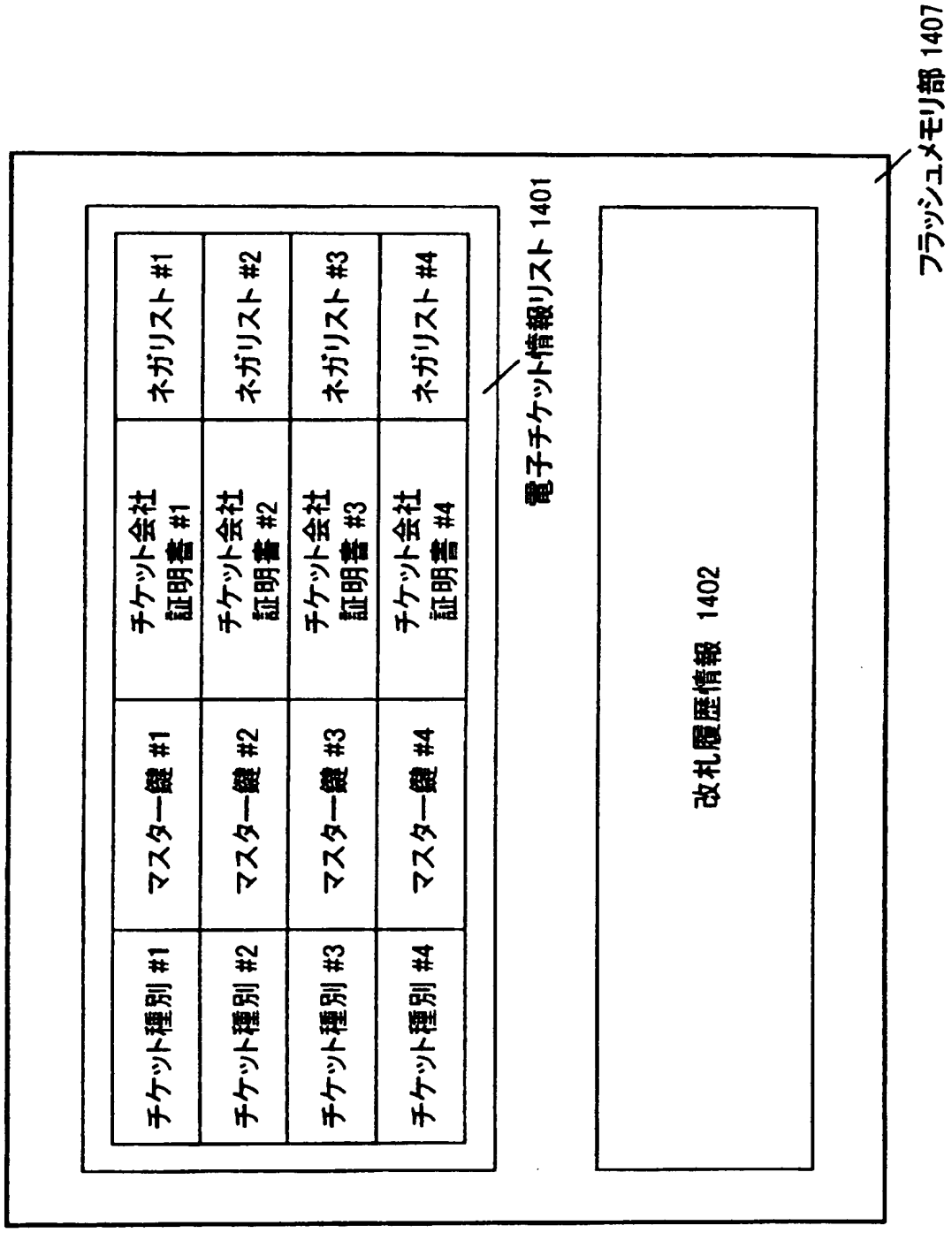
【図１２】



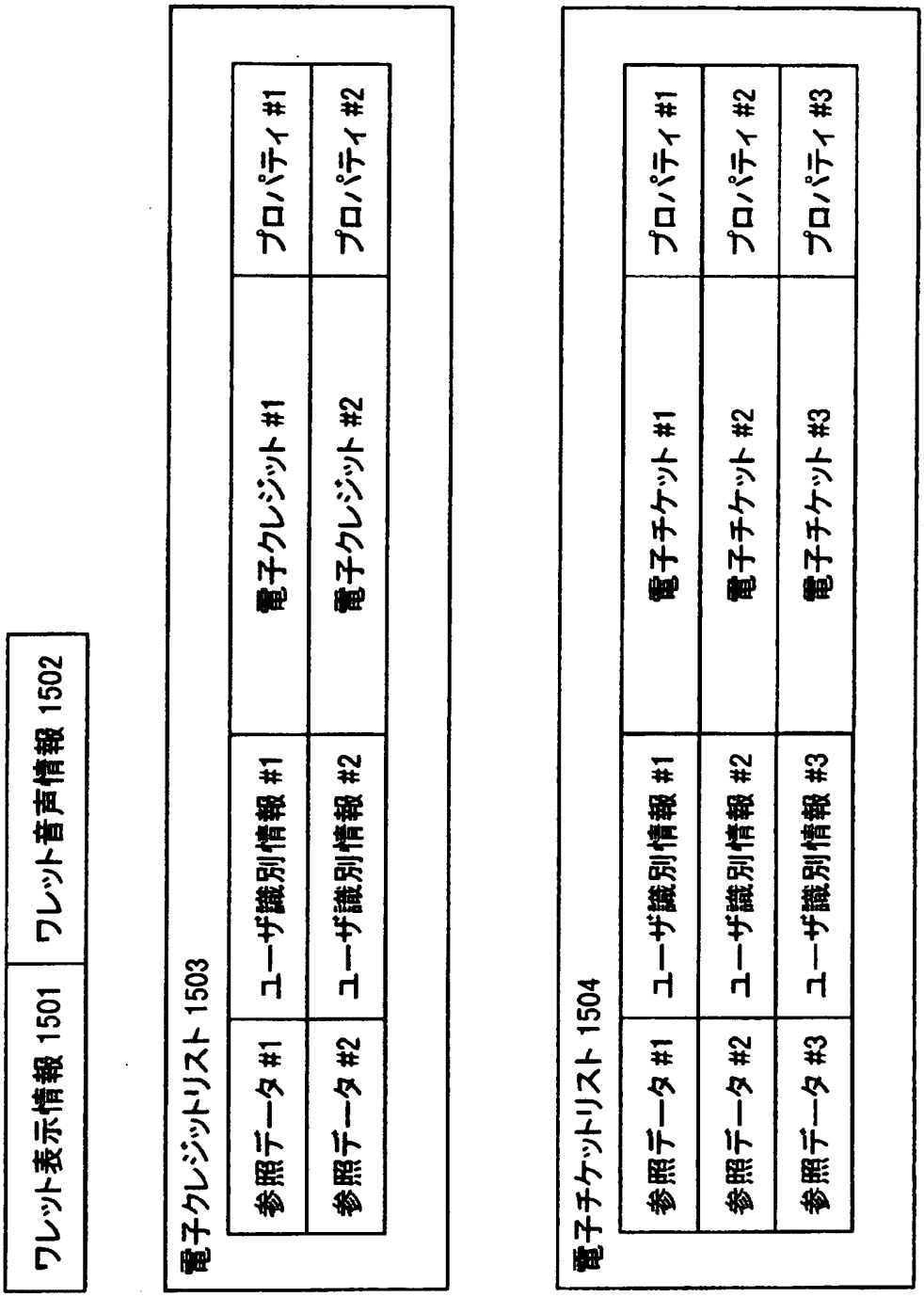
【図１３】


制御部 1310
セキュリティモジュール 1300
TRM部 1306
CPU 1301
ROM 1302
RAM 1303
EEPROM 1304
コ・プロセッサ 1305
フラッシュメモリ部 1307
ゲート機構部 1311
起動センサー 1312
ローカルワイヤレス通信I/F 1313
LED 1314
スピーカ 1315

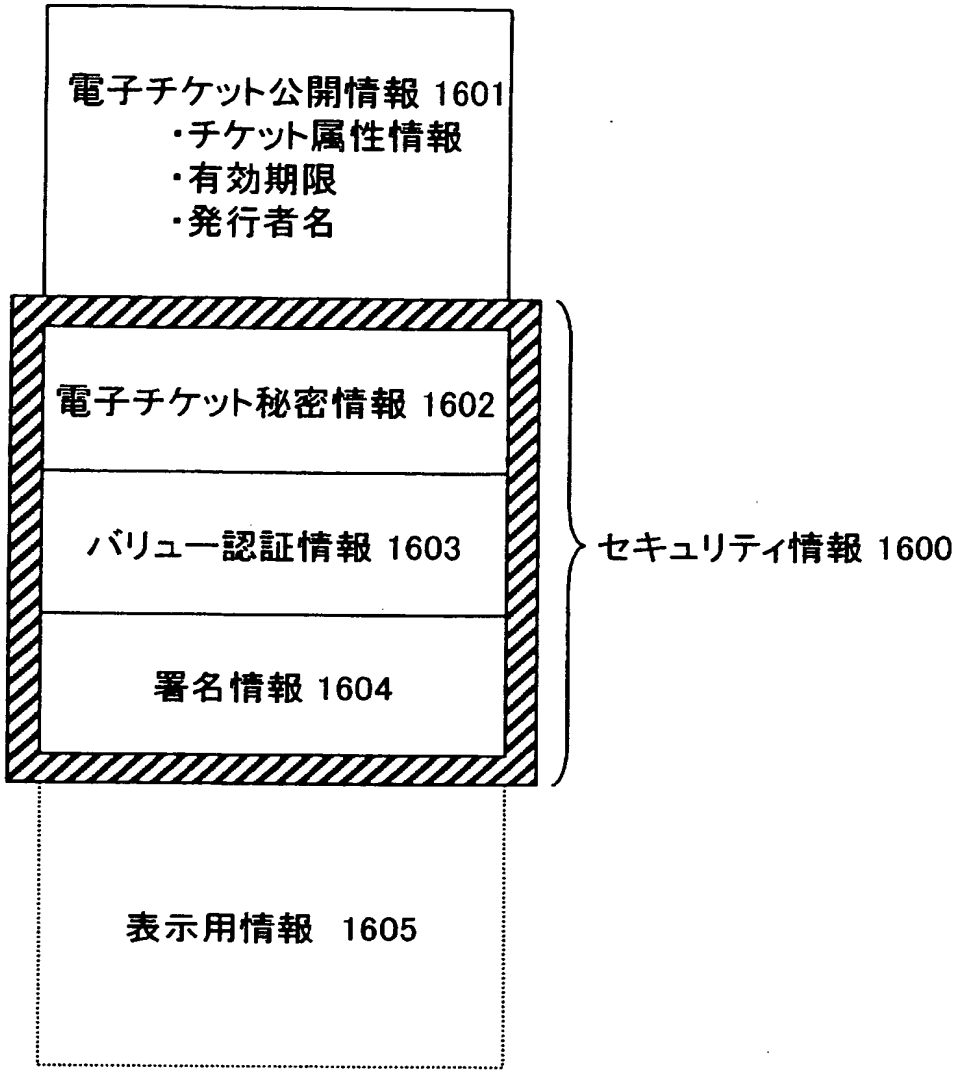
【図１４】


フラッシュメモリ部 1407
電子チケット情報リスト 1401
チケット種別 #1
マスター鍵 #1
チケット会社 証明書 #1
ネガリスト #1
チケット種別 #2
マスター鍵 #2
チケット会社 証明書 #2
ネガリスト #2
チケット種別 #3
マスター鍵 #3
チケット会社 証明書 #3
ネガリスト #3
チケット種別 #4
マスター鍵 #4
チケット会社 証明書 #4
ネガリスト #4
改札履歴情報 1402

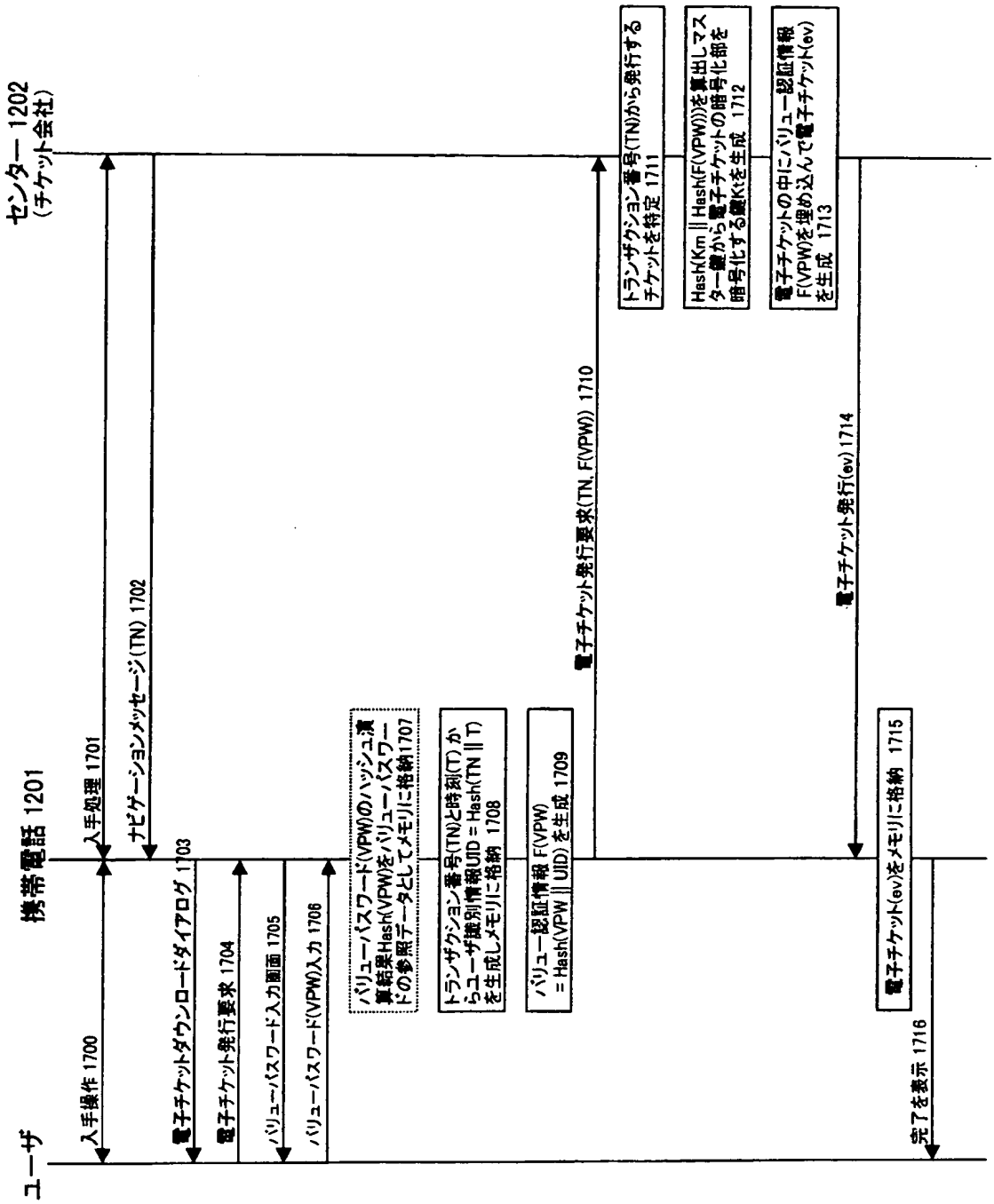
【図１５】


ワレット表示情報 1501
ワレット音声情報 1502
電子クレジットリスト 1503
参照データ #1
ユーザ識別情報 #1
電子クレジット #1
プロパティ #1
参照データ #2
ユーザ識別情報 #2
電子クレジット #2
プロパティ #2
電子チケットリスト 1504
参照データ #1
ユーザ識別情報 #1
電子チケット #1
プロパティ #1
参照データ #2
ユーザ識別情報 #2
電子チケット #2
プロパティ #2
参照データ #3
ユーザ識別情報 #3
電子チケット #3
プロパティ #3

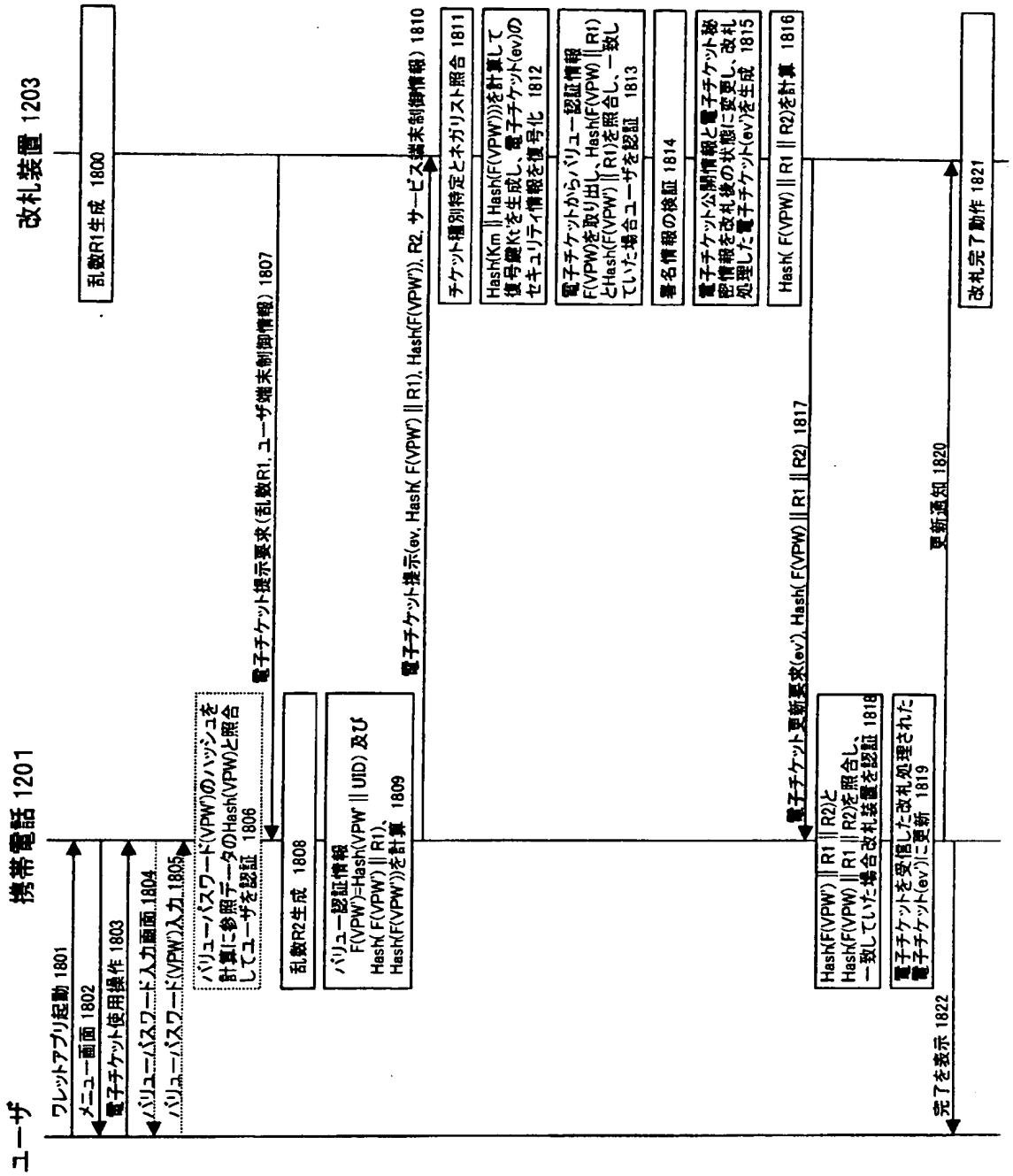
【図１６】


電子チケット公開情報 1601
・チケット属性情報
・有効期限
・発行者名
電子チケット秘密情報 1602
バリュー認証情報 1603
署名情報 1604
セキュリティ情報 1600
表示用情報　1605

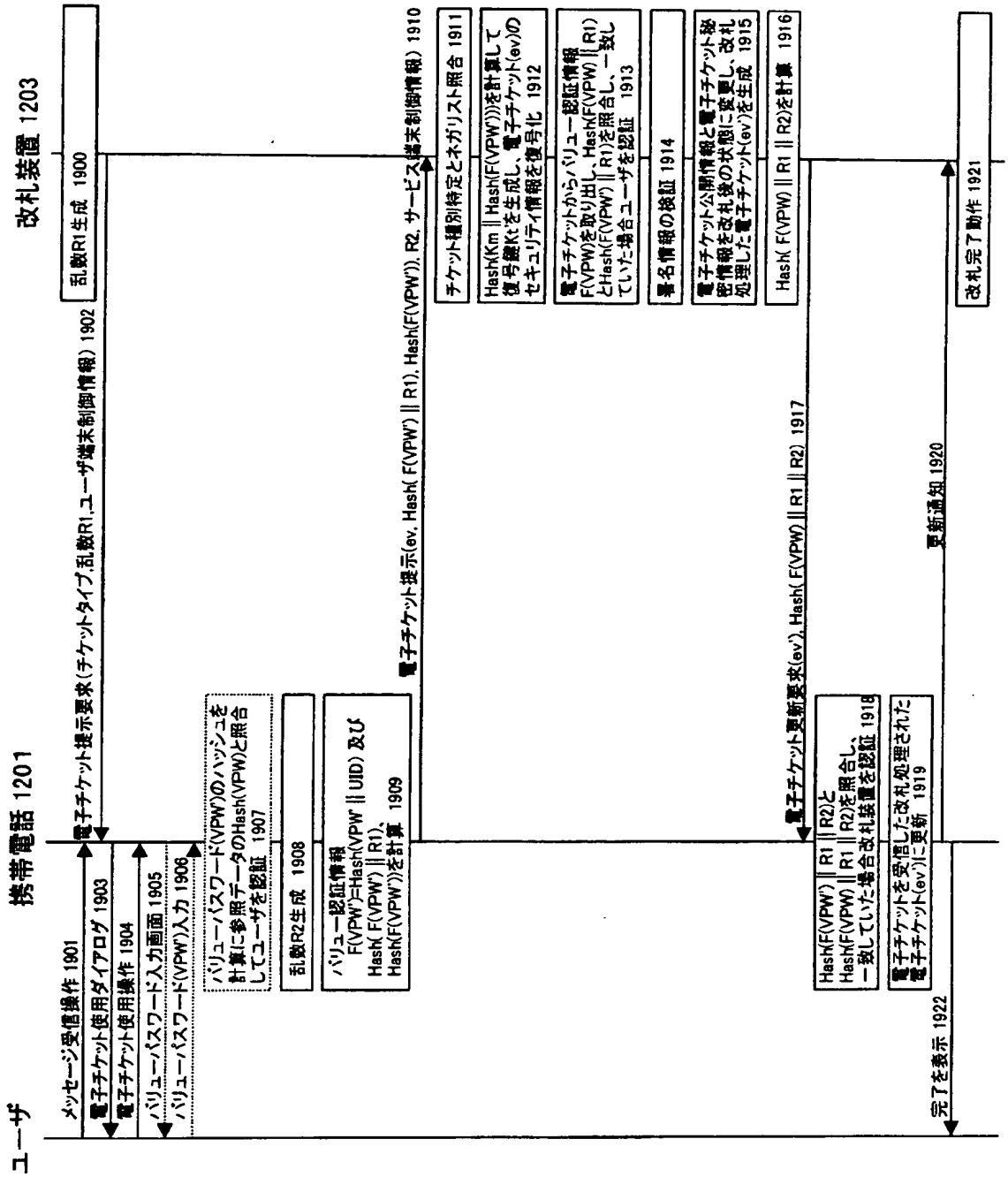
【図１７】


センター 1202
(チケット会社)
携帯電話 1201
ユーザ
入手処理 1701
ナビゲーションメッセージ(TN) 1702
電子チケットダウンロードダイアログ 1703
電子チケット発行要求 1704
パリューパスワード入力画面 1705
パリューパスワード(VPW)入力 1706
パリューパスワード(VPW)のハッシュ演算結果Hash(VPW)をパリューパスワードの参照データとしてメモリに格納1707
トランザクション番号(TN)と時刻(T)からユーザ識別情報(UID = Hash(TN ‖ T)を生成しメモリに格納 1708
パリュー認証情報 F(VPW) = Hash(VPW ‖ UID) を生成 1709
電子チケット発行要求(TN, F(VPW)) 1710
トランザクション番号(TN)から発行するチケットを特定 1711
Hash(Km ‖ Hash(F(VPW)))を真出しマスター鍵から電子チケットの暗号化部を暗号化する鍵Kを生成 1712
電子チケットの中にパリュー認証情報F(VPW)を埋め込んで電子チケット(ev)を生成 1713
電子チケット発行(ev) 1714
電子チケット(ev)をメモリに格納 1715
完了を表示 1716
入手操作 1700

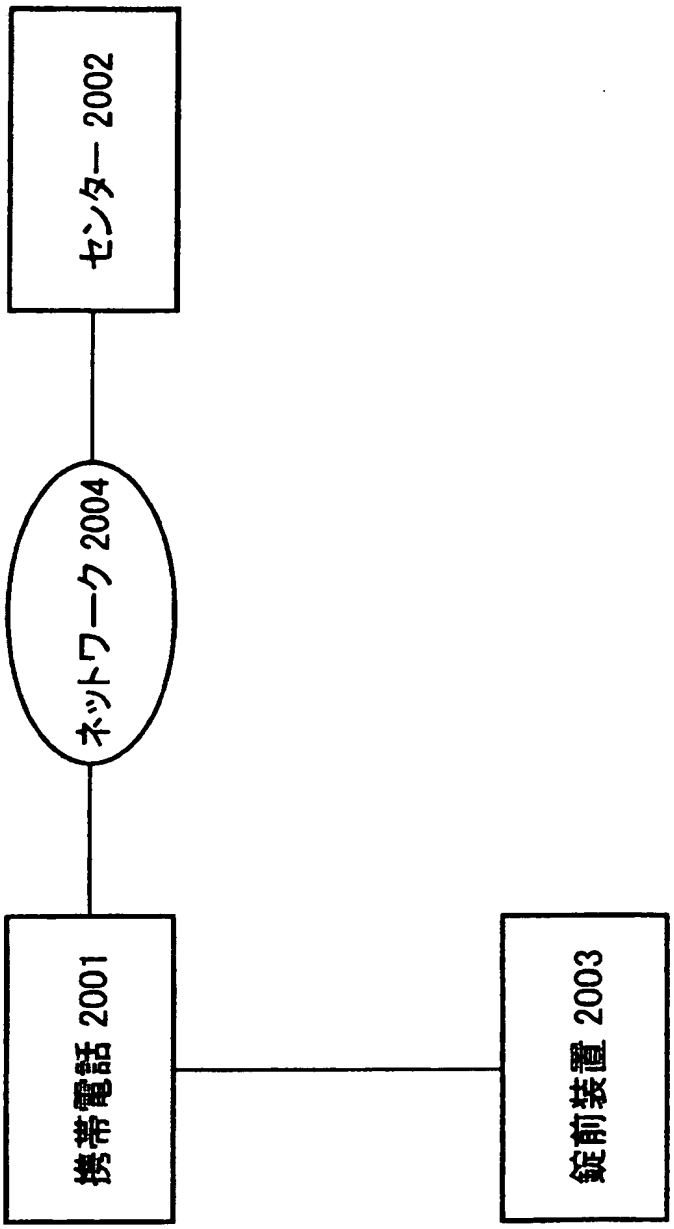
【図１８】


ユーザ
携帯電話 1201
改札装置 1203
フレットアプリ起動 1801
メニュー画面 1802
電子チケット使用操作 1803
パリューパスワード入力画面 1804
パリューパスワード(VPW)入力 1805
乱数R1生成 1800
パリューパスワード(VPW')のハッシュを計算に参照データのHash(VPW)と照合してユーザを認証 1806
電子チケット提示要求(乱数R1, ユーザ端末制御情報) 1807
乱数R2生成 1808
パリュー認証情報 F(VPW')=Hash(VPW' || UID) 及び Hash(F(VPW') || R1), Hash(F(VPW'))を計算 1809
電子チケット提示(ev, Hash(F(VPW') || R1), Hash(F(VPW')), R2, サービス端末制御情報) 1810
チケット種別特定とネガリスト照合 1811
Hash(Km || Hash(F(VPW')))を計算して復号鍵Kt'を生成し、電子チケット(ev)のセキュリティ情報を復号化 1812
電子チケットからパリュー認証情報 F(VPW)を取り出し、Hash(F(VPW) || R1)とHash(F(VPW') || R1)を照合し、一致していた場合ユーザを認証 1813
署名情報の検証 1814
電子チケット公開情報と電子チケット秘密情報を改札後の状態に変更し、改札処理した電子チケット(ev')を生成 1815
Hash(F(VPW) || R1 || R2)を計算 1816
電子チケット更新要求(ev'), Hash(F(VPW) || R1 || R2) 1817
Hash(F(VPW') || R1 || R2)とHash(F(VPW) || R1 || R2)を照合し、一致していた場合改札装置を認証 1818
電子チケットを受信した改札処理された電子チケット(ev')に更新 1819
更新通知 1820
改札完了動作 1821
完了を表示 1822

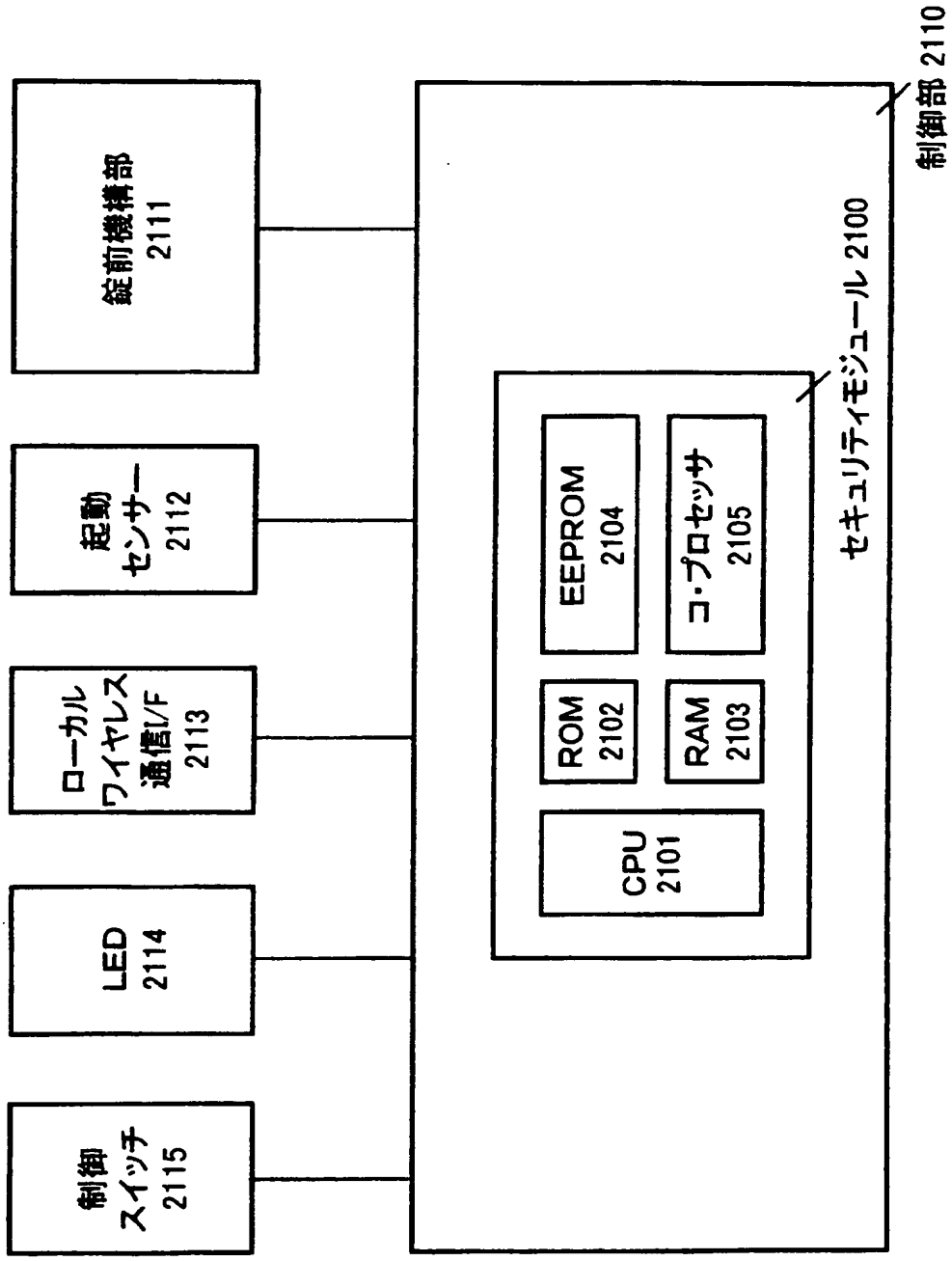
【図１９】


ユーザ
携帯電話 1201
改札装置 1203
メッセージ受信操作 1901
電子チケット使用ダイアログ 1903
電子チケット使用操作 1904
パリューパスワード入力画面 1905
パリューパスワード(VPW')入力 1906
乱数R1生成 1900
電子チケット提示要求(チケットタイプ,乱数R1,ユーザ端末制御情報) 1902
パリューパスワード(VPW')のハッシュを計算に参照データのHash(VPW)と照合してユーザを認証 1907
乱数R2生成 1908
パリュー認証情報 F(VPW')=Hash(VPW' || UID) 及び Hash(F(VPW') || R1), Hash(F(VPW'))を計算 1909
電子チケット提示(ev, Hash(F(VPW') || R1), Hash(F(VPW')), R2, サービス端末制御情報) 1910
チケット種別特定とネガリスト照合 1911
Hash(Km || Hash(F(VPW')))を計算して復号鍵Kcを生成し、電子チケット(ev)のセキュリティ情報を復号化 1912
電子チケットからパリュー認証情報 F(VPW)を取り出し、Hash(F(VPW) || R1) とHash(F(VPW') || R1)を照合し、一致していた場合ユーザを認証 1913
署名情報の検証 1914
電子チケット公開情報と電子チケット秘密情報を改札後の状態に変更し、改札処理した電子チケット(ev')を生成 1915
Hash(F(VPW) || R1 || R2)を計算 1916
電子チケット更新要求(ev'), Hash(F(VPW) || R1 || R2) 1917
Hash(F(VPW') || R1 || R2)とHash(F(VPW) || R1 || R2)を照合し、一致していた場合改札操作を認証 1918
電子チケットを受信した改札処理された電子チケット(ev')に更新 1919
更新通知 1920
改札完了動作 1921
完了を表示 1922

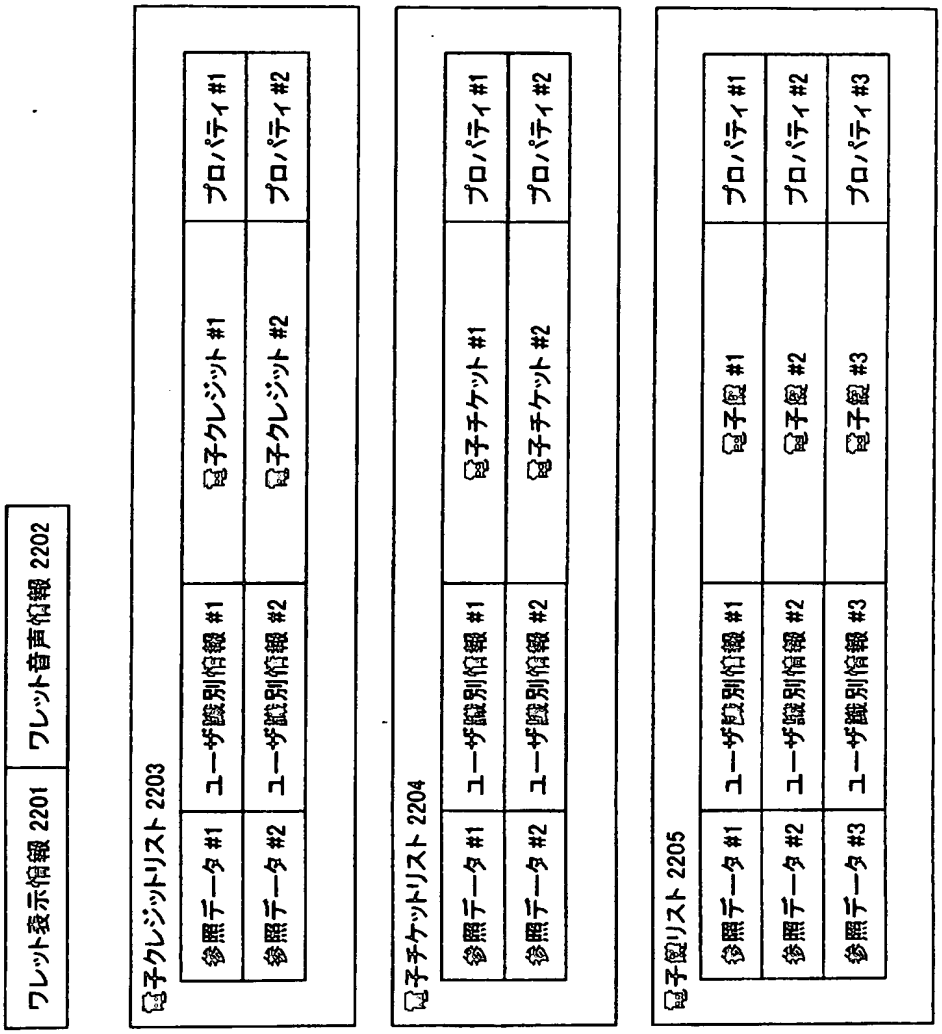
【図２０】



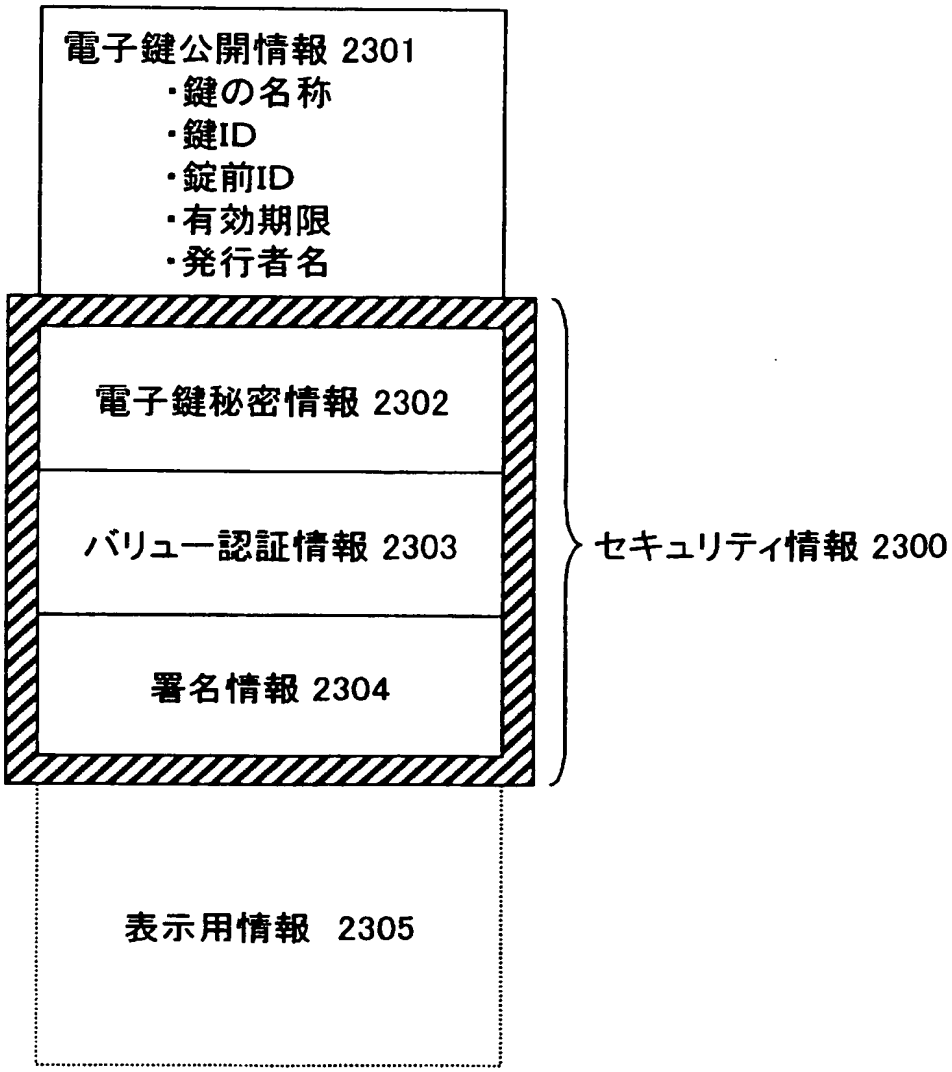
【図２１】


錠前機構部
2111
起動
センサー
2112
ローカル
ワイヤレス
通信I/F
2113
LED
2114
制御
スイッチ
2115
制御部 2110
セキュリティモジュール 2100
EEPROM
2104
コ・プロセッサ
2105
ROM
2102
RAM
2103
CPU
2101

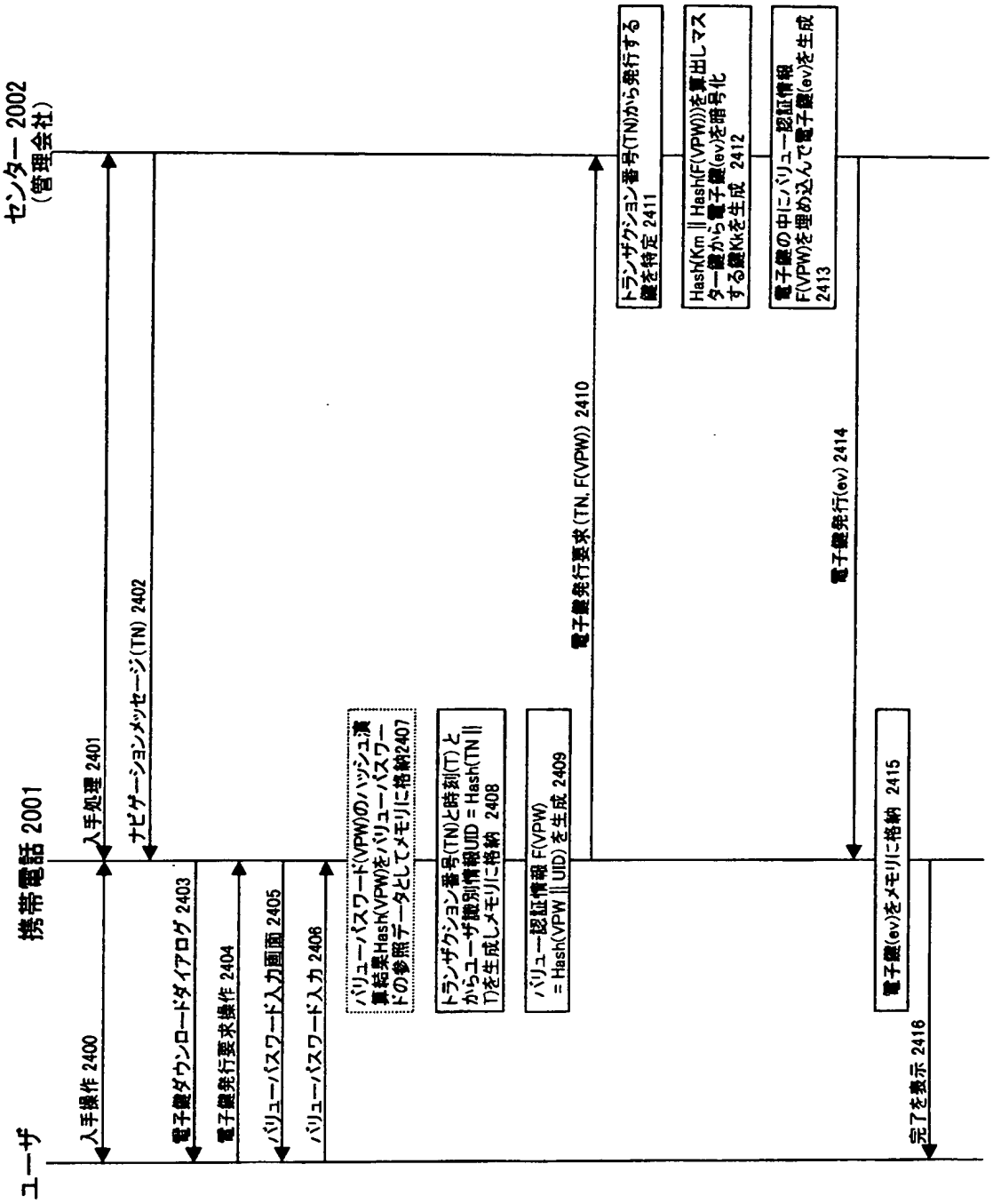
【図２２】


フレット表示情報 2201
フレット音声情報 2202
子クレジットリスト 2203
参照データ #1
ユーザ識別情報 #1
子クレジット #1
プロパティ #1
参照データ #2
ユーザ識別情報 #2
子クレジット #2
プロパティ #2
子チケットリスト 2204
参照データ #1
ユーザ識別情報 #1
子チケット #1
プロパティ #1
参照データ #2
ユーザ識別情報 #2
子チケット #2
プロパティ #2
子役リスト 2205
参照データ #1
ユーザ識別情報 #1
子役 #1
プロパティ #1
参照データ #2
ユーザ識別情報 #2
子役 #2
プロパティ #2
参照データ #3
ユーザ識別情報 #3
子役 #3
プロパティ #3

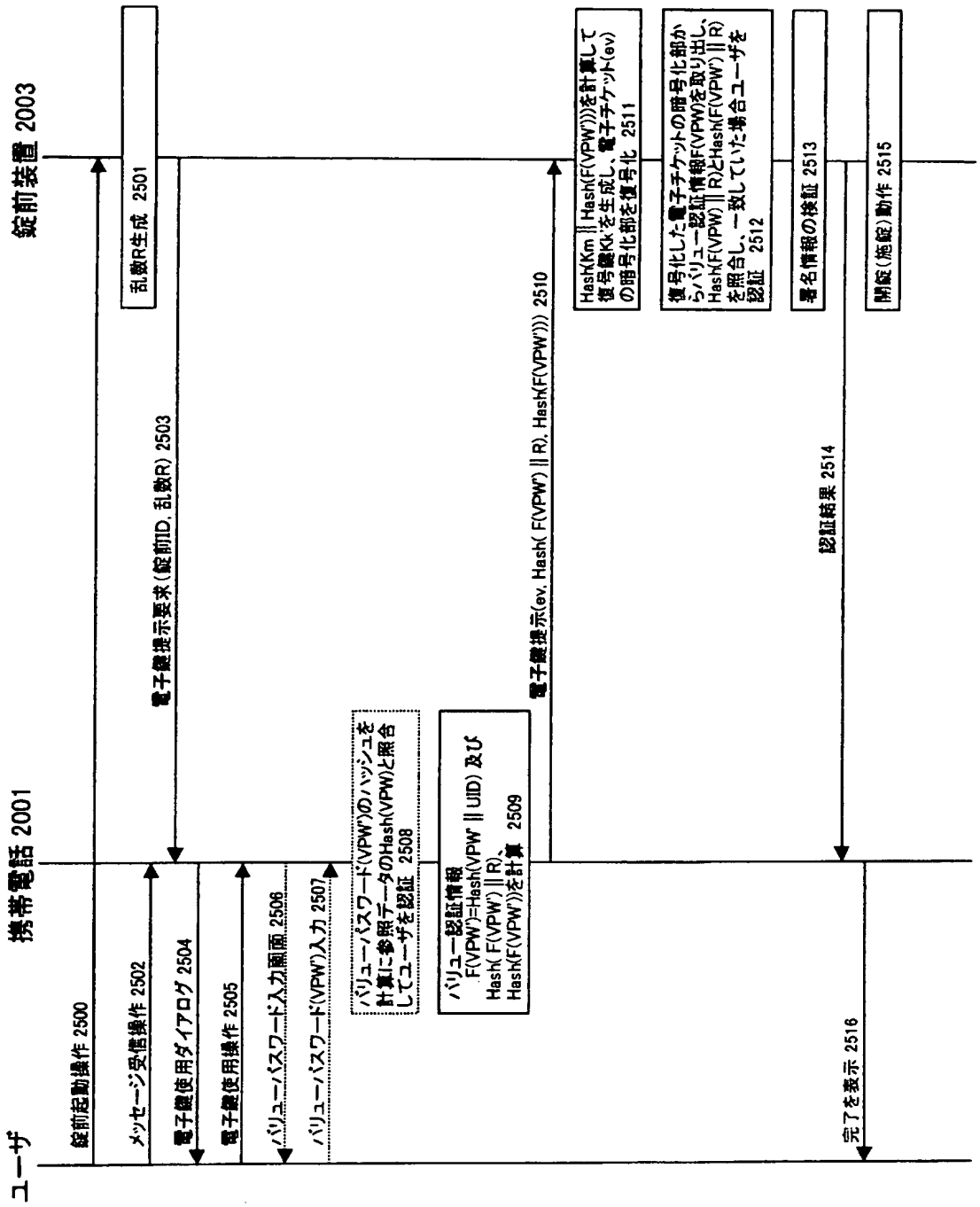
【図２３】


電子鍵公開情報 2301
・鍵の名称
・鍵ID
・錠前ID
・有効期限
・発行者名
電子鍵秘密情報 2302
バリュー認証情報 2303
署名情報 2304
セキュリティ情報 2300
表示用情報　2305

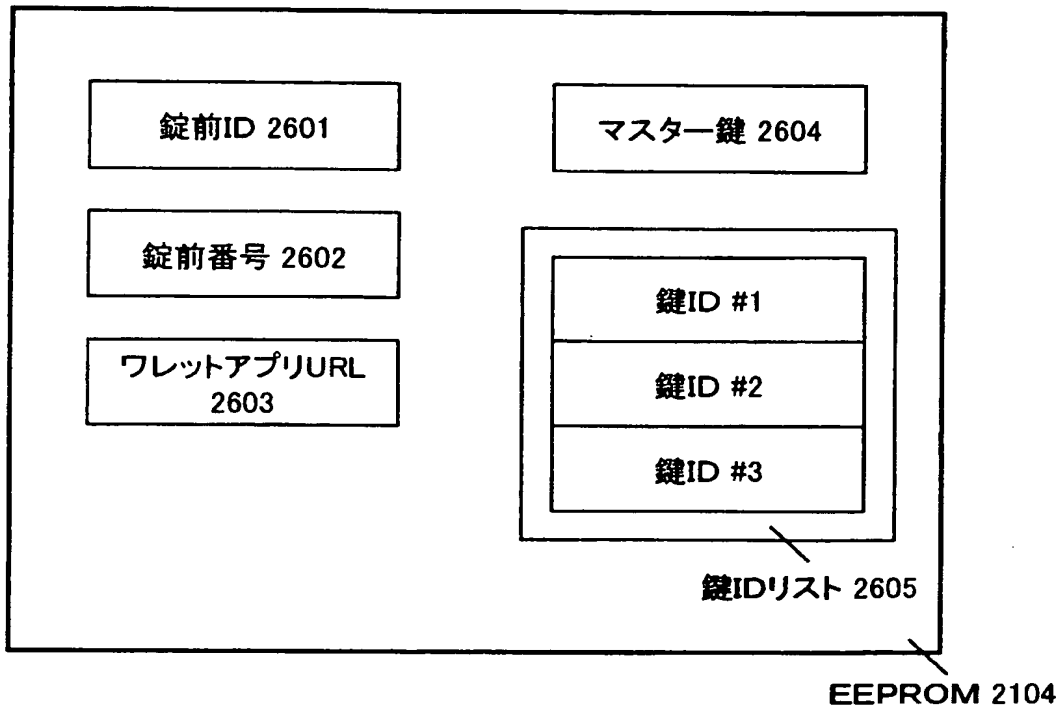
【図２４】


センター 2002
(管理会社)
携帯電話 2001
ユーザ
入手処理 2401
ナビゲーションメッセージ(TN) 2402
入手操作 2400
電子鍵ダウンロードダイアログ 2403
電子鍵発行要求操作 2404
バリューパスワード入力画面 2405
バリューパスワード入力 2406
バリューパスワード(VPW)のハッシュ演算結果Hash(VPW)をバリューパスワードの参照データとしてメモリに格納2407
トランザクション番号(TN)と時刻(T)とからユーザ識別情報UID = Hash(TN || T)を生成しメモリに格納 2408
バリュー認証情報 F(VPW) = Hash(VPW || UID)を生成 2409
電子鍵発行要求(TN, F(VPW)) 2410
トランザクション番号(TN)から発行する鍵を特定 2411
Hash(Km || Hash(F(VPW)))を真出しマスター鍵から電子鍵(ev)を暗号化する鍵Kkを生成 2412
電子鍵の中にバリュー認証情報F(VPW)を埋め込んで電子鍵(ev)を生成 2413
電子鍵発行(ev) 2414
電子鍵(ev)をメモリに格納 2415
完了を表示 2416

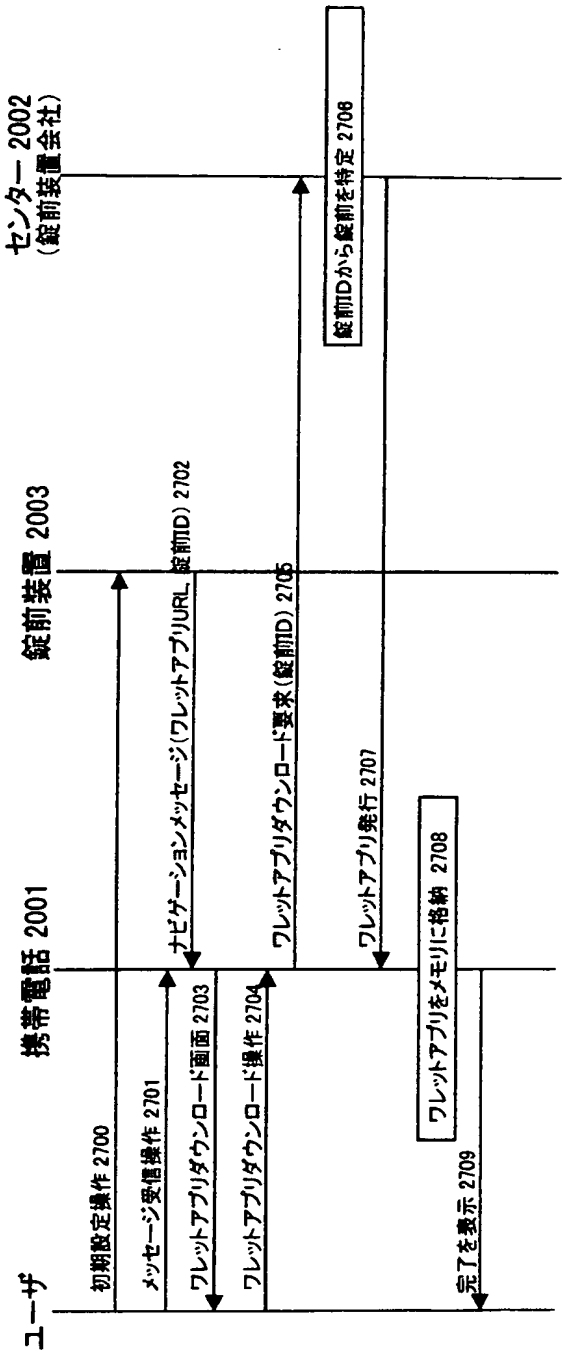
【図２５】


ユーザ
携帯電話 2001
錠前装置 2003
錠前起動操作 2500
メッセージ受信操作 2502
電子鍵使用ダイアログ 2504
電子鍵使用操作 2505
バリューパスワード入力画面 2506
バリューパスワード(VPW')入力 2507
バリューパスワード(VPW')のハッシュを計算に参照データのHash(VPW)と照合してユーザを認証 2508
バリュー認証情報 F(VPW')=Hash(VPW' || UID) 及び Hash(F(VPW') || R)、 Hash(F(VPW'))を計算 2509
乱数R生成 2501
電子鍵提示要求(錠前ID, 乱数R) 2503
電子鍵提示(ev, Hash(F(VPW') || R), Hash(F(VPW'))) 2510
Hash(Km || Hash(F(VPW')))を計算して復号鍵Kkを生成し、電子チケット(ev)の暗号化部を復号化 2511
復号化した電子チケットの暗号化部からバリュー認証情報F(VPW')を取り出し、Hash(F(VPW') || R)とHash(F(VPW') || R)を照合し、一致していた場合ユーザを認証 2512
署名情報の検証 2513
認証結果 2514
閉錠(施錠)動作 2515
完了を表示 2516

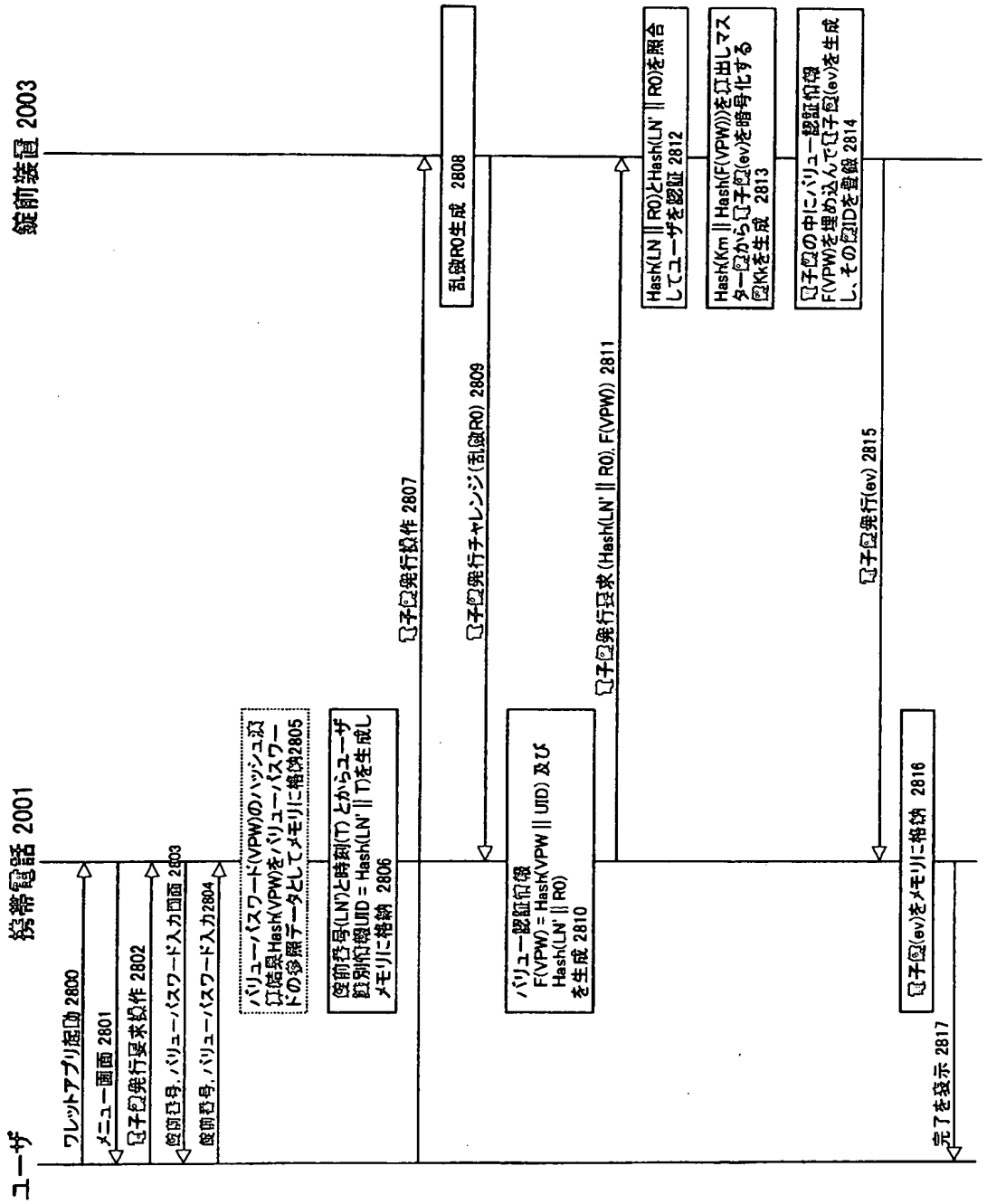
【図２６】


錠前ID 2601
マスター鍵 2604
錠前番号 2602
ワレットアプリURL 2603
鍵ID #1
鍵ID #2
鍵ID #3
鍵IDリスト 2605
EEPROM 2104

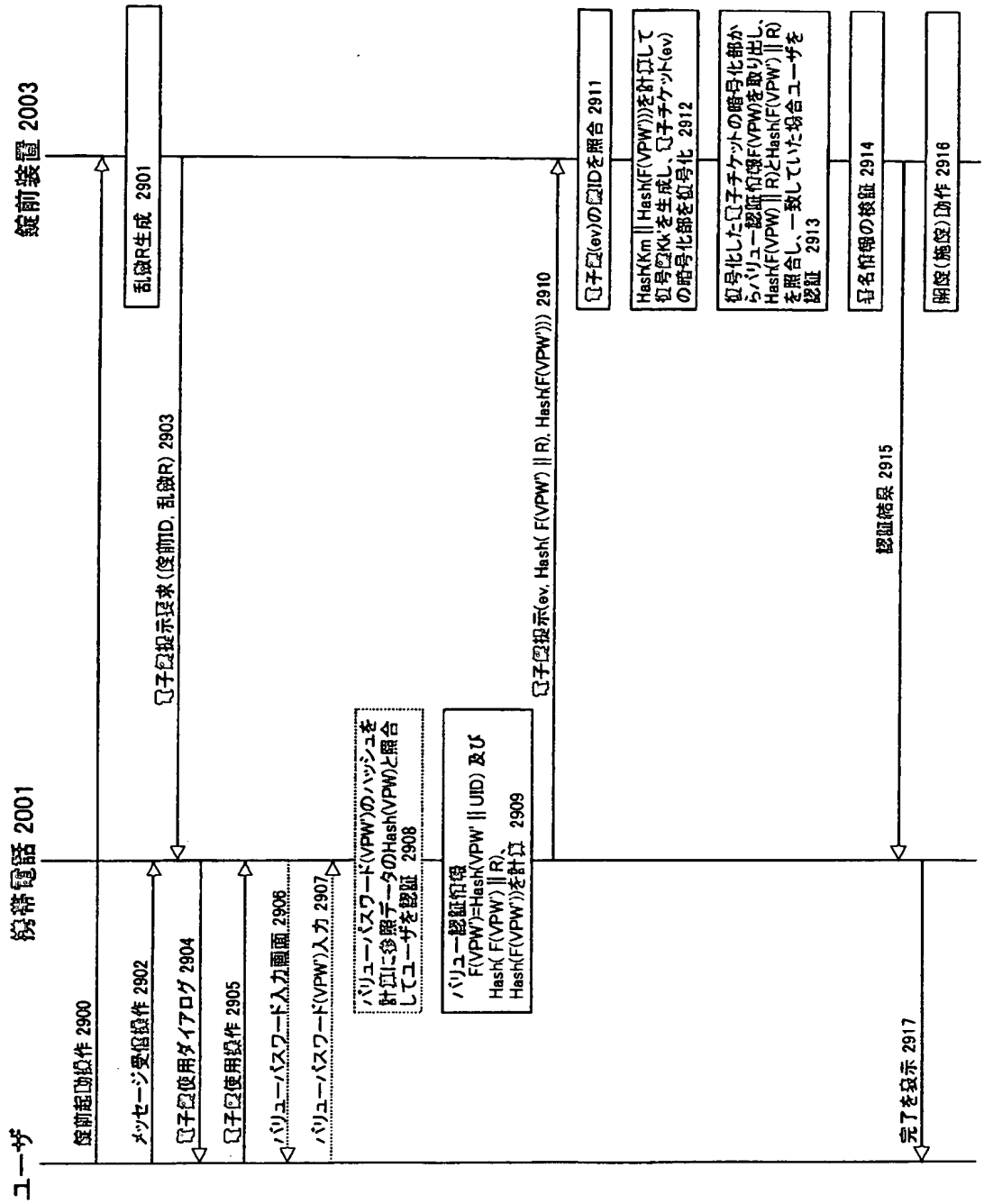
【図２７】


センター 2002
(錠前装置会社)
錠前装置 2003
携帯電話 2001
ユーザ
初期設定操作 2700
メッセージ受信操作 2701
ナビゲーションメッセージ(ワレットアプリURL 錠前ID) 2702
ワレットアプリダウンロード画面 2703
ワレットアプリダウンロード操作 2704
ワレットアプリダウンロード要求(錠前ID) 2705
錠前IDから錠前を特定 2706
ワレットアプリ発行 2707
ワレットアプリをメモリに格納 2708
完了を表示 2709

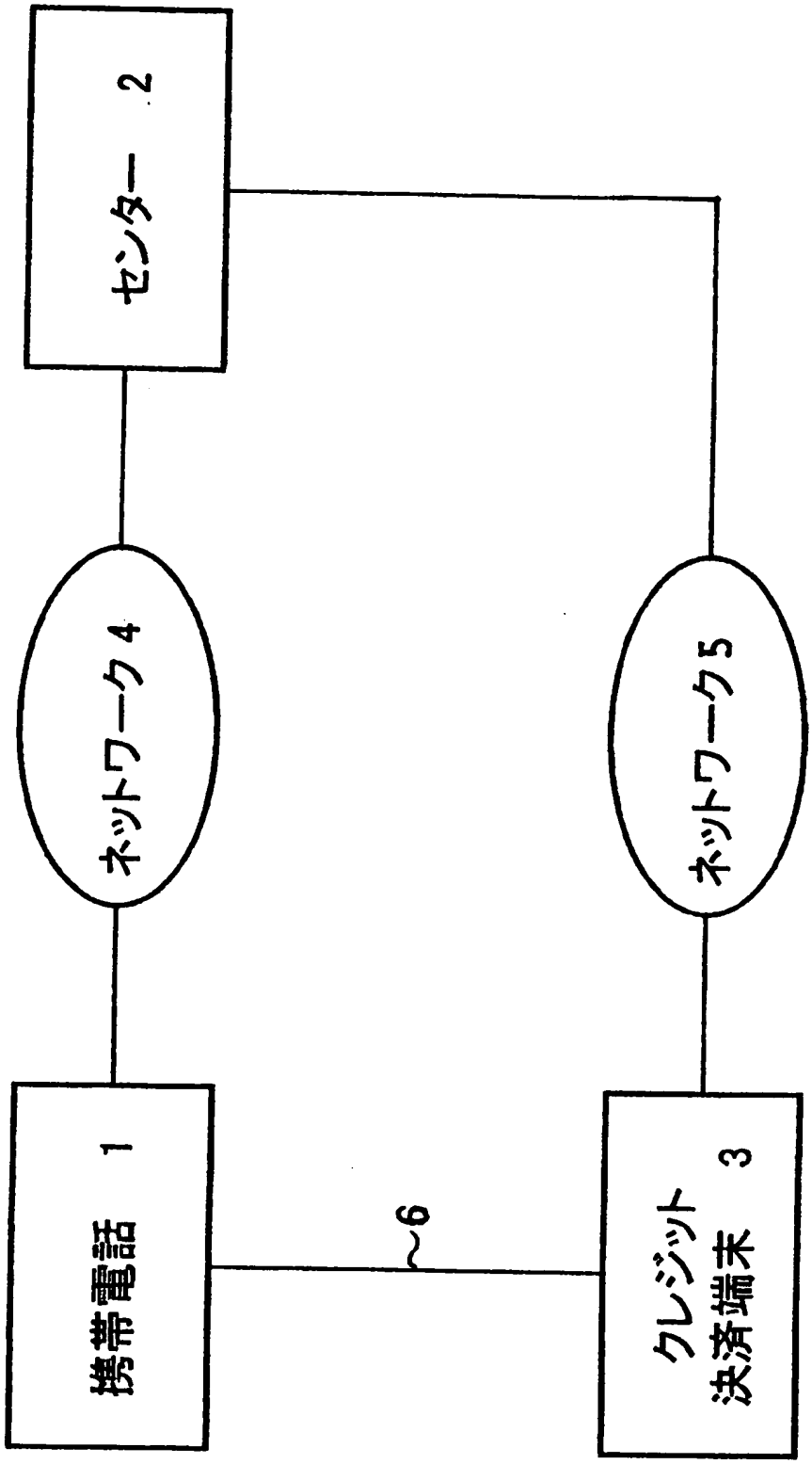
【図２８】


ユーザ
携帯電話 2001
錠前装置 2003
ウレットアプリ起動 2800
メニュー画面 2801
子鍵発行要求操作 2802
登録番号、パリューパスワード入力画面 2803
登録番号、パリューパスワード入力2804
パリューパスワード(VPW)のハッシュ値
結果Hash(VPW)をパリューパスワードの登録データとしてメモリに格納2805
登録番号(LN')と時刻(T)とからユーザ識別情報UID = Hash(LN' || T)を生成しメモリに格納 2806
子鍵発行操作 2807
乱数R0生成 2808
子鍵発行チャレンジ(乱数R0) 2809
パリュー認証情報
F(VPW) = Hash(VPW || UID) 及び
Hash(LN' || R0)
を生成 2810
子鍵発行要求(Hash(LN' || R0), F(VPW)) 2811
Hash(LN || R0)とHash(LN' || R0)を照合してユーザを認証 2812
Hash(Km || Hash(F(VPW)))を出しマスター鍵から子鍵(ev)を暗号化するKkを生成 2813
子鍵の中にパリュー認証情報F(VPW)を埋め込んで子鍵(ev)を生成し、その鍵IDを登録 2814
子鍵発行(ev) 2815
子鍵(ev)をメモリに格納 2816
完了を表示 2817

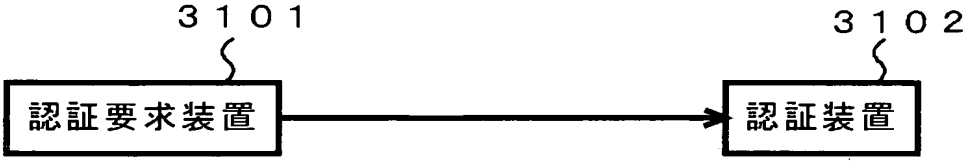
【図２９】


ユーザ
携帯電話 2001
錠前装置 2003
使前起動操作 2900
メッセージ受信操作 2902
子鍵使用ダイアログ 2904
子鍵使用操作 2905
パリューパスワード入力画面 2906
パリューパスワード(VPW')入力 2907
パリューパスワード(VPW')のハッシュを計算に参照データのHash(VPW)と照合してユーザを認証 2908
パリュー認証情報 F(VPW')=Hash(VPW' || UID) 及び Hash(F(VPW') || R), Hash(F(VPW'))を計算 2909
乱数R生成 2901
子鍵提示要求(使前ID, 乱数R) 2903
子鍵提示(ev, Hash(F(VPW') || R), Hash(F(VPW'))) 2910
子鍵(ev)の鍵IDを照合 2911
Hash(Km || Hash(F(VPW')))を計算して鍵情報Kmを生成し、子チケット(ev)の暗号化部を鍵暗号化 2912
鍵暗号化した子チケットの暗号化部からパリュー認証情報F(VPW)を取り出し、Hash(F(VPW) || R)とHash(F(VPW') || R)を照合し、一致していた場合ユーザを認証 2913
名前情報の検証 2914
認証結果 2915
開錠(施錠)動作 2916
完了を表示 2917

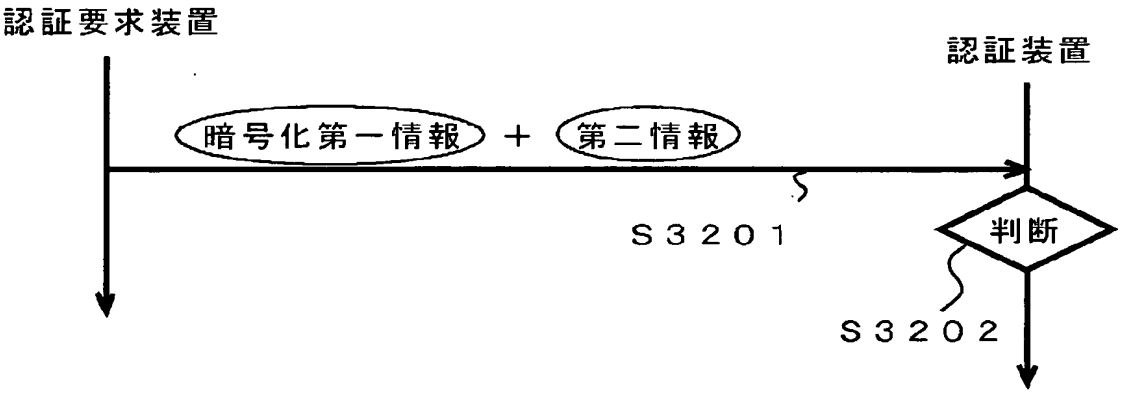
【図３０】



【図３１】


３１０１
３１０２
認証要求装置
認証装置

【図３２】


認証要求装置
認証装置
暗号化第一情報
＋
第二情報
Ｓ３２０１
判断
Ｓ３２０２

【図３３】

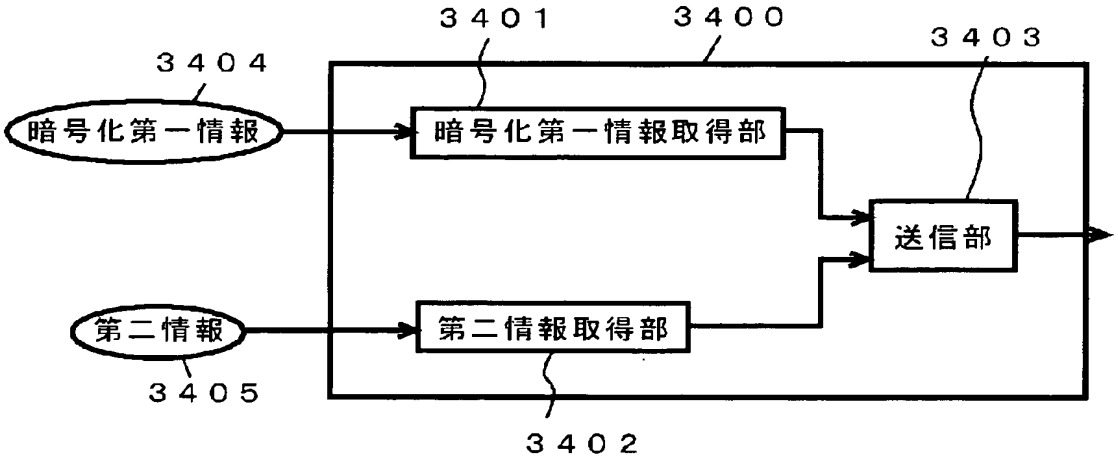
（Ａ）

暗号化第一情報	Encypt（パスワード）
第二情報	パスワード
判断の条件	Decrypt（暗号化第一情報）＝第二情報？

（Ｂ）

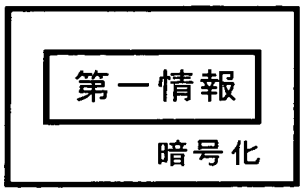
暗号化第一情報	Encypt（パスワード）
第二情報	F（パスワード）
判断の条件	F(Decrypt（暗号化第一情報））＝第二情報？

【図３４】

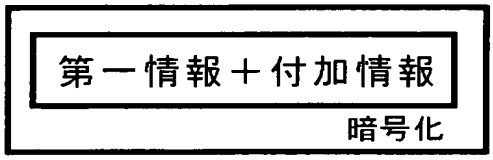


【図３５】

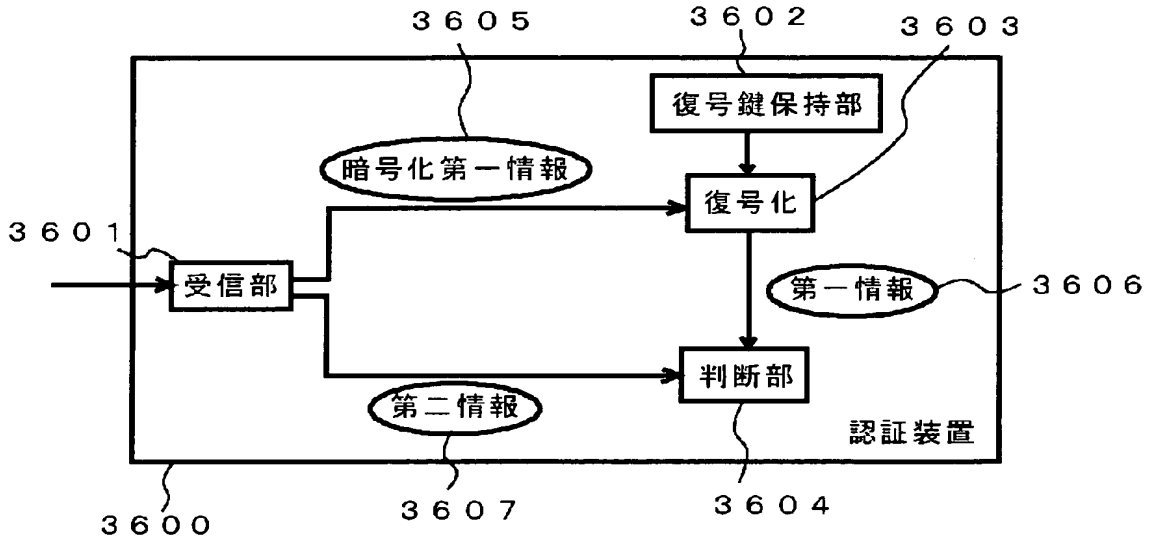
（Ａ）


第一情報
暗号化

（Ｂ）

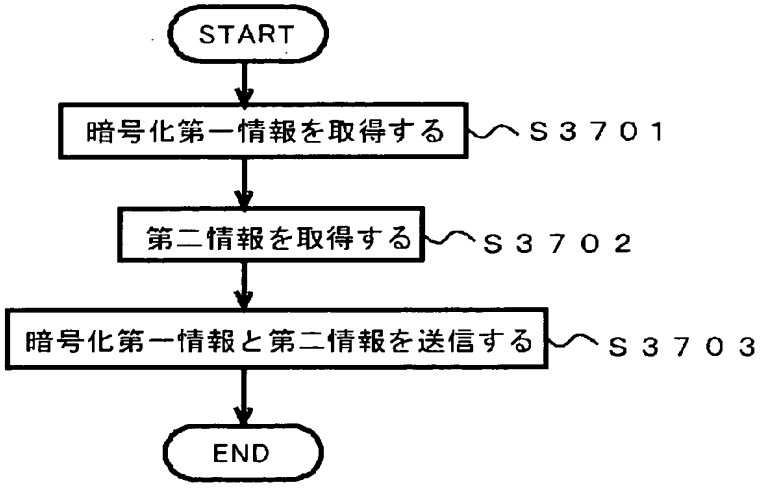

第一情報＋付加情報
暗号化

【図３６】

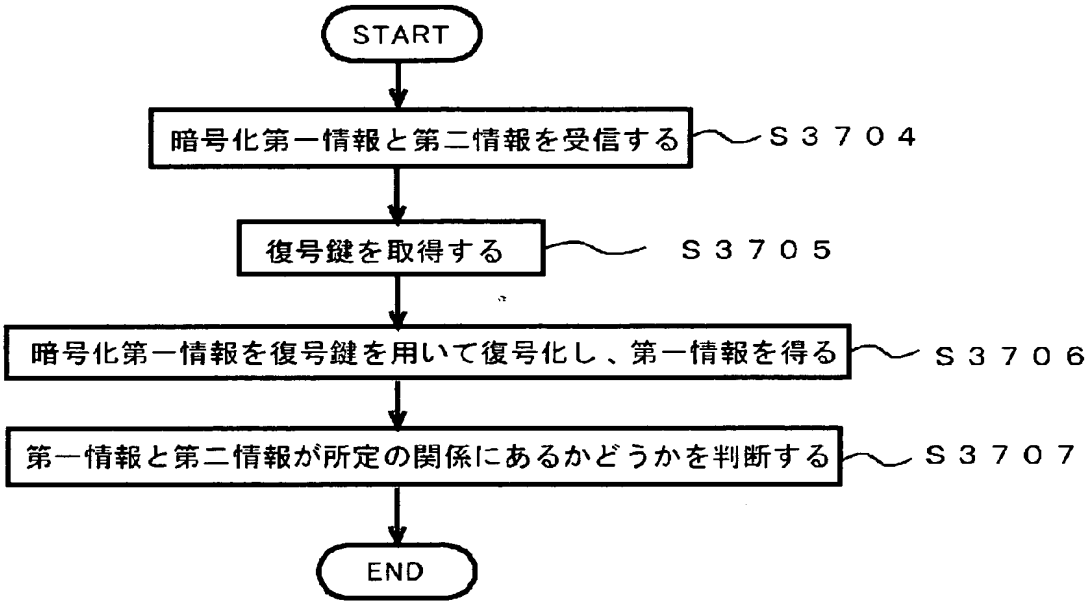

３６０５
３６０２
３６０３
復号鍵保持部
暗号化第一情報
復号化
３６０１
受信部
第一情報
３６０６
判断部
第二情報
認証装置
３６００
３６０７
３６０４

【図３７】

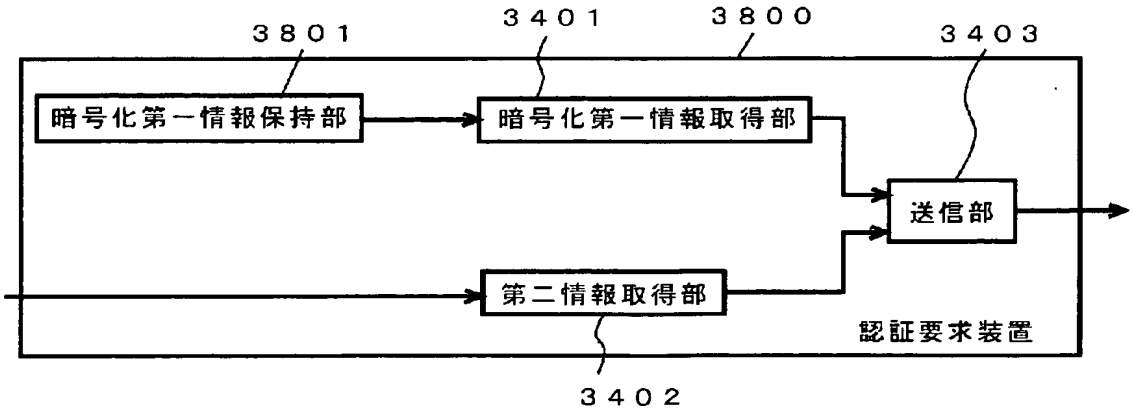
（Ａ）


START
暗号化第一情報を取得する
Ｓ３７０１
第二情報を取得する
Ｓ３７０２
暗号化第一情報と第二情報を送信する
Ｓ３７０３
END

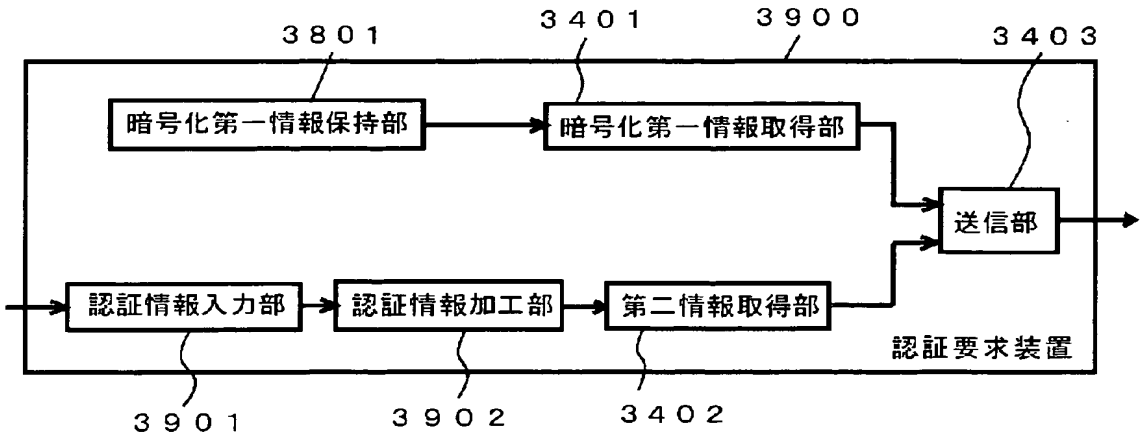
（Ｂ）


START
暗号化第一情報と第二情報を受信する
Ｓ３７０４
復号鍵を取得する
Ｓ３７０５
暗号化第一情報を復号鍵を用いて復号化し、第一情報を得る
Ｓ３７０６
第一情報と第二情報が所定の関係にあるかどうかを判断する
Ｓ３７０７
END

【図３８】

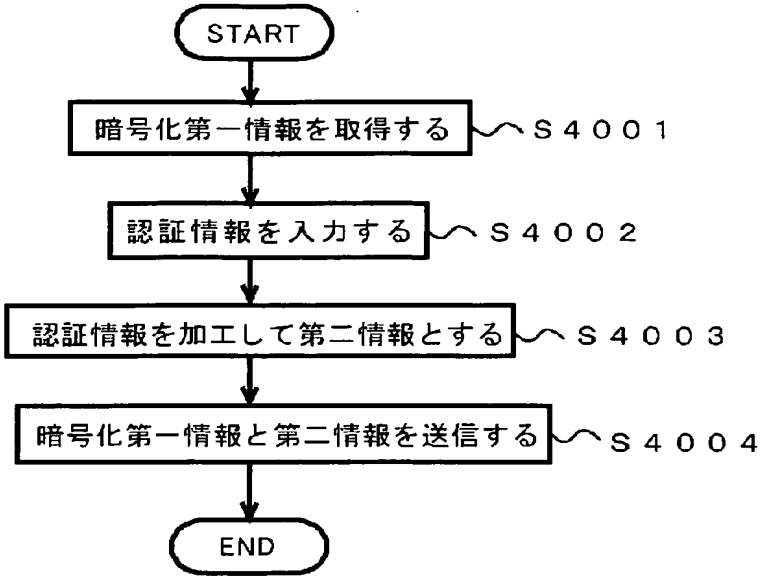

３８０１
３４０１
３８００
３４０３
暗号化第一情報保持部
暗号化第一情報取得部
送信部
第二情報取得部
認証要求装置
３４０２

【図３９】

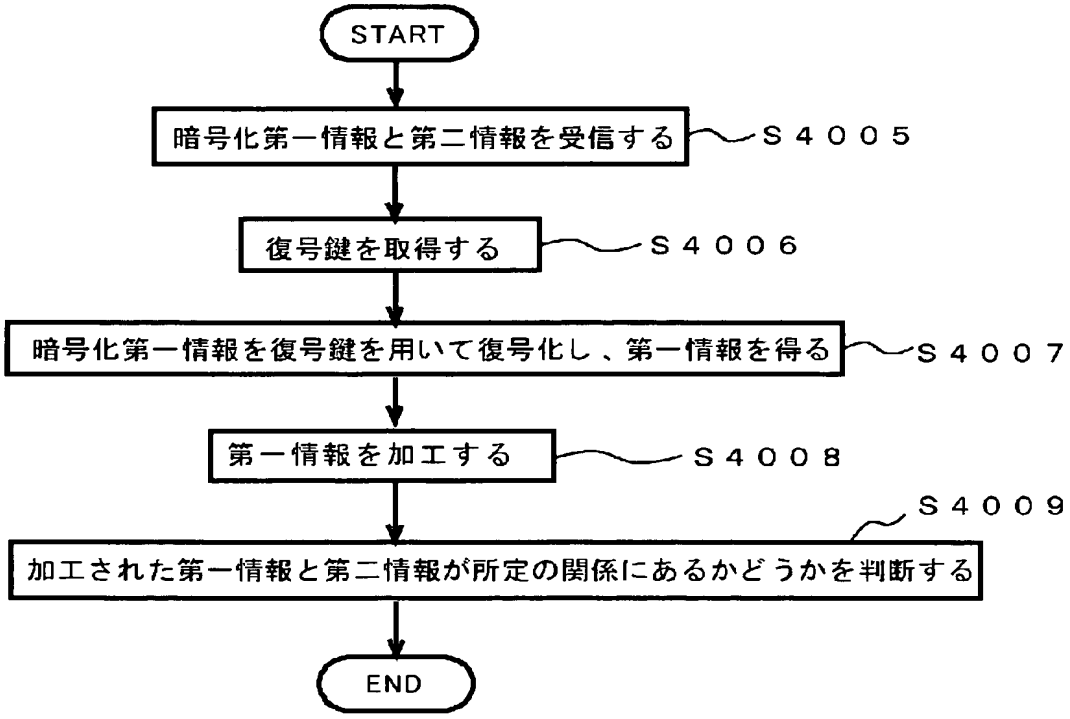

３８０１
３４０１
３９００
３４０３
暗号化第一情報保持部
暗号化第一情報取得部
送信部
認証情報入力部
認証情報加工部
第二情報取得部
認証要求装置
３９０１
３９０２
３４０２

【図４０】

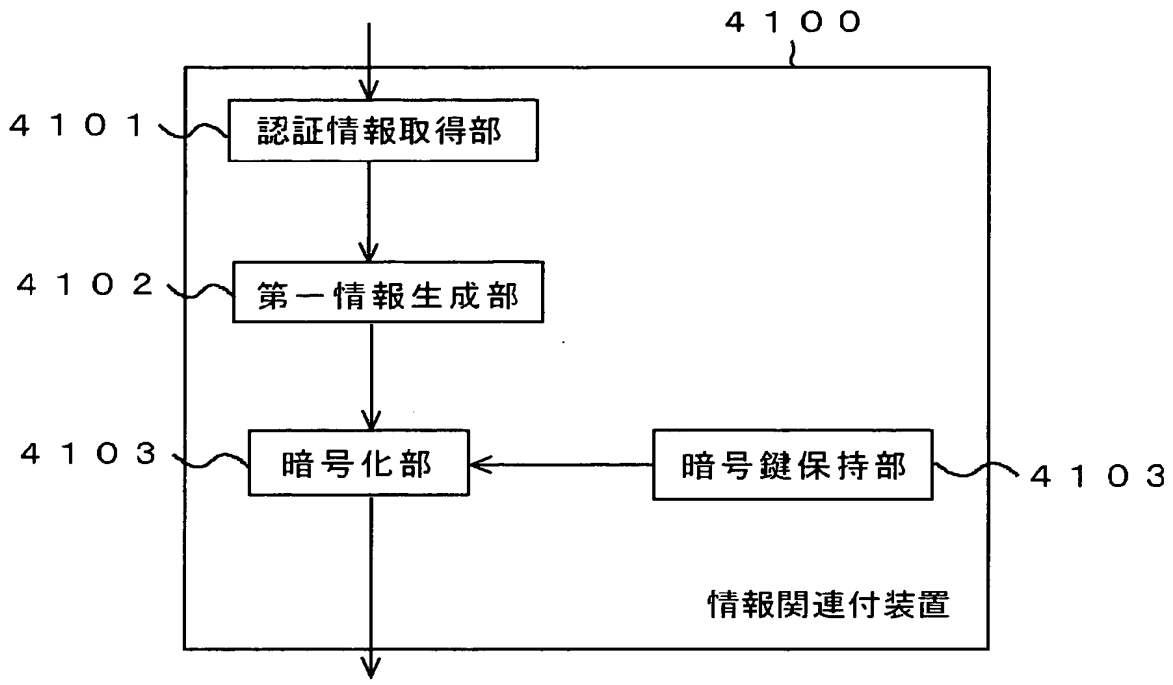
（Ａ）


START
暗号化第一情報を取得する
Ｓ４００１
認証情報を入力する
Ｓ４００２
認証情報を加工して第二情報とする
Ｓ４００３
暗号化第一情報と第二情報を送信する
Ｓ４００４
END

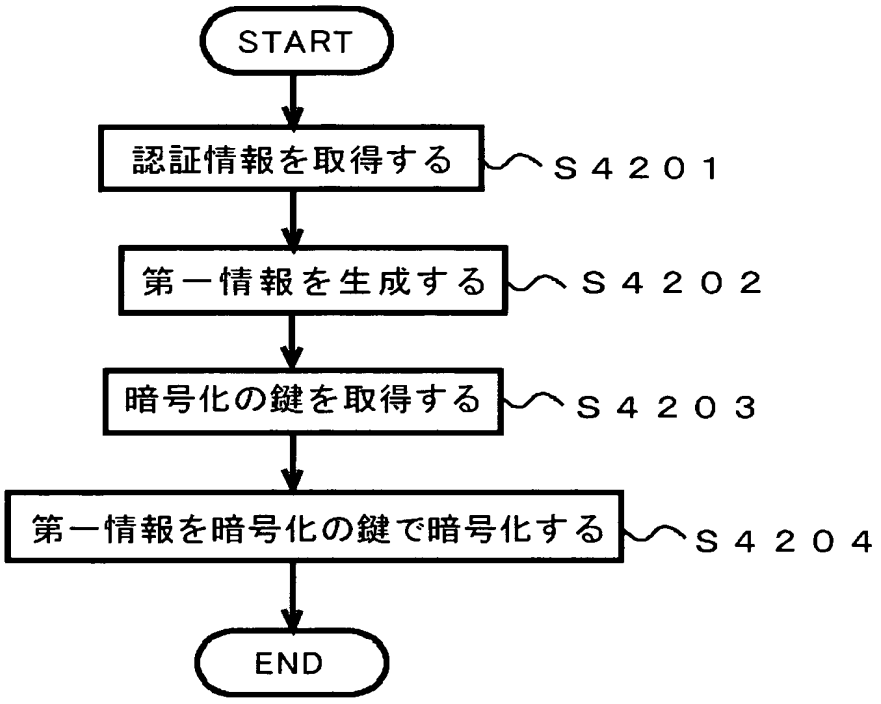
（Ｂ）


START
暗号化第一情報と第二情報を受信する
Ｓ４００５
復号鍵を取得する
Ｓ４００６
暗号化第一情報を復号鍵を用いて復号化し、第一情報を得る
Ｓ４００７
第一情報を加工する
Ｓ４００８
Ｓ４００９
加工された第一情報と第二情報が所定の関係にあるかどうかを判断する
END

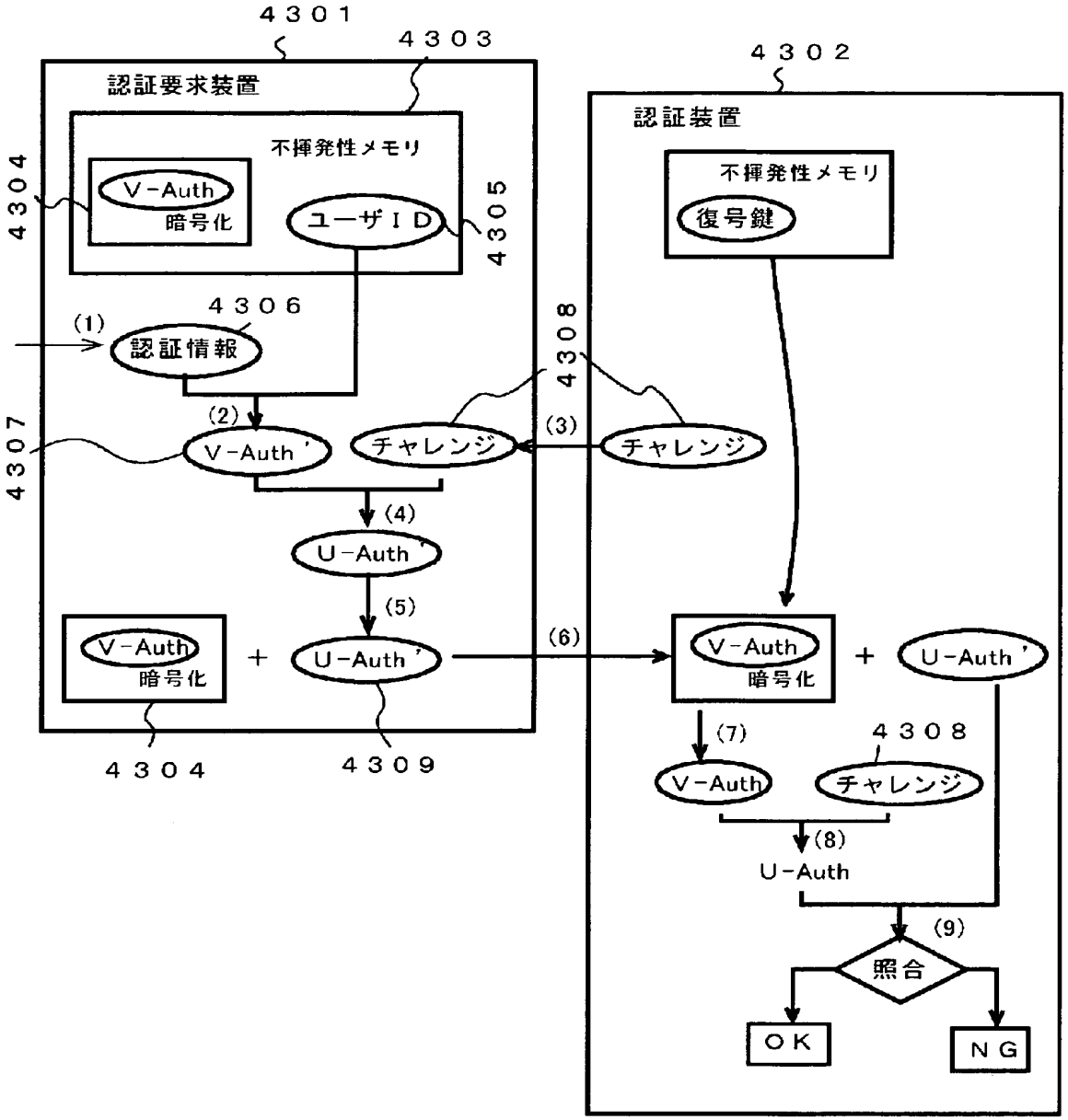
【図４１】


４１００
４１０１
認証情報取得部
４１０２
第一情報生成部
４１０３
暗号化部
暗号鍵保持部
４１０３
情報関連付装置

【図４２】


START
認証情報を取得する
Ｓ４２０１
第一情報を生成する
Ｓ４２０２
暗号化の鍵を取得する
Ｓ４２０３
第一情報を暗号化の鍵で暗号化する
Ｓ４２０４
END

【図４３】



【図４４】

$V\text{-}Auth = Hash_1$（パスワード ‖ ユーザID）

（２） $V\text{-}Auth' = Hash_1$（認証情報 ‖ ユーザID）

（４） $U\text{-}Auth' = Hash_2$（$V\text{-}Auth'$ ‖ チャレンジ）

（８） $U\text{-}Auth = Hash_2$（$V\text{-}Auth'$ ‖ チャレンジ）

【書類名】要約書
【要約】
【課題】　耐タンパ機能のない携帯端末であっても、電子バリューの安全な認証処理が出来る認証システムを提供する。
【解決手段】　ユーザの携帯端末に格納された電子バリューにはユーザが指定した認証情報(VPW)にハッシュ演算を施したバリュー認証情報(F(VPW))が暗号化されて含まれている。ユーザを認証する際は、認証装置が乱数Rを携帯端末に送信し、携帯端末はユーザが入力した認証情報(VPW')からバリュー認証情報(F(VPW'))を生成し、乱数Rと組み合わせたデータにハッシュ演算を行い認証情報Hash(F(VPW')|| R)を生成して、電子バリューと共に認証装置に送信し、認証装置は、受信した電子バリューの暗号を復号化して、バリュー認証情報(F(VPW))を取り出し、乱数Rと組み合わせたデータにハッシュ演算を行い認証情報Hash(F(VPW)|| R)を生成し、受信した認証情報Hash(F(VPW')|| R)と認証情報Hash(F(VPW)|| R)とが一致することを検証して、ユーザを認証する。
【選択図】　図１０

認定・付加情報

特許出願の番号	特願２００３－２８９４３３
受付番号	５０３０１３１５８８１
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　８月１２日

＜認定情報・付加情報＞

【提出日】　平成15年 8月 7日

特願２００３－２８９４３３

出　願　人　履　歴　情　報

識別番号　　［０００００５８２１］

１．変更年月日　　１９９０年　８月２８日
［変更理由］　　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社